LOAN DOCUMENT

PHOTOGRAPH THIS SHEET

TJAGSA

(1)

LEVEL

INVENTORY

DTIC ACCESSION NUMBER

Information Operations and Warfare: . . .

DOCUMENT IDENTIFICATION

May 97

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DISTRIBUTION STATEMENT

HANDLE WITH CARE

ACCESSION FOR

NTIS GRA&I ☐
DTIC TRAC ☐
UNANNOUNCED ☐
JUSTIFICATION

BY

DISTRIBUTION/

AVAILABILITY CODES

DISTRIBUTION	AVAILABILITY AND/OR SPECIAL	
A-1		

DISTRIBUTION STAMP

DATE ACCESSIONED

DATE RETURNED

20060105 021

DATE RECEIVED IN DTIC

REGISTERED OR CERTIFIED NUMBER

PHOTOGRAPH THIS SHEET AND RETURN TO DTIC-FDAC

DTIC FORM 70A JUN 90

DOCUMENT PROCESSING SHEET

PREVIOUS EDITIONS MAY BE USED UNTIL STOCK IS EXHAUSTED.

LOAN DOCUMENT

INFORMATION OPERATIONS AND WARFARE: FUNDAMENTAL CHALLENGES FOR THE 21ST CENTURY

A Thesis
Presented To
The Judge Advocate General's School
United States Army

The opinions and conclusions expressed herein are those of the author and do not necessarily represent the views of either The Judge Advocate General's School, The United States Army, or any other governmental agency.

by Captain Catherine M. With

United States Army

45th Judge Advocate Graduate Course

May 1997

ABSTRACT

Information technology is rapidly evolving and altering the manner in which our nation engages the world community. As our past experiences in international law demonstrate, this another tool in the military technology evolution which has not alterd the basic fundamental principles of law and warfare in our present international law paradigm. The current international law framework can be applied effectively to information operations and warfare. This is accomplished by employing an "incrementalist view" of international law. Such an approach pursues incremental, evolutionary changes and revisions in a current framework in order to adapt to the changing environment. A framework for analysis within the current international law model is easily developed and used. Additionally, employing the "net effect" principle, which works within the current legal paradigm and focuses upon the intent and result of an information operation, makes it possible to determine the legality of information operations.

Table of Contents

INFORMATION OPERATIONS AND WARFARE: FUNDAMENTAL CHALLENGES FOR THE 21st CENTURY

CAPTAIN CATHERINE M. WITH*

Everything in this world, including money, operates not on reality – but on the perceptions of reality . . . The world is not run by weapons anymore – or energy or money – it is run by little ones and zeroes, little bits of data, it is all just electrons . . . . There is a war out there, old friend, a world war. And it is not about who's got the most bullets – it's about who controls the information: what we see and hear, how we work, what we think. It's all about the information.[1]

I. Introduction

The dawning of the 21st Century introduces myriad challenges created by the worldwide explosion of information technology. The incredibly rapid technological

---

*Judge Advocate General's Corps, United States Army. Presently assigned as Student, 45th Judge Advocate Officer Graduate Course, The Judge Advocate General's School United States Army. M.A., B.A., *summa cum laude*, dual major and dual degree program, 1985, The College of Saint Rose, Albany, New York; J.D., Note & Comment Editor, ALBANY LAW REVIEW, 1988, Albany Law School of Union University, New York; Formerly assigned as Chief, Legal Assistance; Command Judge Advocate, United States Forces Haiti, United Nations Mission in Haiti; Operations Law Attorney, Multinational Force Haiti; Administrative Law Attorney; 25th Infantry Division (Light), Schofield Barracks, Hawaii, 1994-1996; Special Assistant to the Commander-in-Chief, United States Southern Command; Chief, Operations Law Division; Operations Law Attorney; Administrative Law Attorney; Office of the Staff Judge Advocate, Headquarters, U.S. Army South, Republic of Panama, 1991-1994; Command Judge Advocate, Multinational Force and Observers, Sinai, Egypt; Legal Assistance Attorney; and Trial Counsel; Office of the Staff Judge Advocate, 7th Infantry Division (Light), Fort Ord, California, 1989-1991. Previous publication: *A Mother's Right to Recover Damages in New York for Negligent Infliction of Emotional Distress After a Stillbirth - Prognosis: No Recovery?* 53 ALBANY L. REV. 217 (1988). This article is based on a written dissertation that the author submitted to satisfy, in part, the Master of Laws degree requirements for the 45th Judge Advocate Officer Graduate Course.

[1] Excerpts from conversations between the character Cosmo (played by Ben Kingsley) and Martin Bishop (played by Robert Redford), in the 1992 movie SNEAKERS. This movie tells the tale of a maverick surveillance and security team of hackers, led by Martin Bishop, that struggles to retrieve a doomsday-coding machine from a dubious information warfare character named Cosmo. SNEAKERS (Universal 1992).

developments occurring in the collecting, storing, analyzing, and transmitting information greatly affect how the world community conducts business, operates government, and goes through everyday life. While these advancements concerning information are dramatically changing the way people live around the world, of concern to members of the armed forces is how these information technologies are also slowly transforming the way governments interact in peace, crisis, armed conflict, and resolution of conflict.[2] Ultimately, how the world community, especially the international legal community, chooses to analyze and respond to the tremendous information-based challenges will determine our success in employing information operations during the 21st Century.

The technological advances of the Information Age[3] produce futuristic or science fiction type terminology and concepts. Information operations and its subcategory of

---

[2] Peter Grier, *Information Warfare,* AIR FORCE MAG., Mar. 1995, at 34 (hereinafter Grier) ("The explosive development of commercial computers, software, and communications technologies has brought such an electronic 'attack' into the realm of possibility. It does not take the free-floating imagination of a futurist to realize that such breakthroughs as direct-satellite TV broadcasts, morphing software, commercial satellite imagery, and super-computers-on-a-chip all have possible military applications. At a minimum, 'information warfare' means the emergence of greatly improved methods of command, control, and communications. It means thinking about a military organization as a network of networks, rather than a traditional general officer-directed hierarchy.").

[3] The exact date when the Information Age commenced is not certain. The Information Age is best described by the characteristics of the era. "The first day of the Information Age was that day when our dependence upon computers and communications systems and high-tech gadgetry exceeded our ability to live without them." WINN SCHWARTAU, INFORMATION WARFARE: CHAOS ON THE ELECTRONIC SUPERHIGHWAY 59-65 (1994) (hereinafter SCHWARTAU). "The information Age brings with it a host of new inventions: computer networks, internetworks, digital information, information technologies and architectures, and cellular communications; electronic fiscal transactions, information 'highways'; shrinking factories and industrial work forces. Even as quality and productivity increase, new reliable energy generating, sorting and transmitting technologies are transforming the workplace. As the information age matures, others yet-to-be-conceived inventions will continue this

information warfare are popular Information Age topics which present many formidable challenges to modern society.[4] Many writers, scholars, and strategists from both the civilian and military communities continue to contribute a plethora of books and articles about what they believe to be the nature of information operations and information warfare, how they can or should be employed, their importance to the world, and the unique legal issues they

---

transformation and accelerate its pace." General Gordon R. Sullivan and Lieutenant Colonel James M. Dubik, *War in the Information Age*, Strategic Studies Inst., U.S. Army War College, Carlisle Barracks, P.A. (1994). It is the view of authors Douglas H. Dearth and Charles A. Williamson, that it is "the interaction of the information and the knowledge explosions, along with attendant developments in telecommunications and micro-processing technology, and basic demographic trends that produce the defining characteristics of the Information Age." Douglas H. Dearth & Charles A. Williamson, *Information Age/Information War, in* CYBERWAR: SECURITY, STRATEGY, AND CONFLICT IN THE INFORMATION AGE, 13 (Alan D. Campen, et al. eds, 1996).

[4] Dr. Thomas Rona, a preeminent intellectual in the field of information operations, is credited with developing the term "information warfare" in 1976. *See* Thomas P. Rona, *Information Warfare: An Age-old Concept with New Insights,* DEF. INTEL. J., Spring 1996, at 53. Information operations is the term the Department of Defense (DoD) started using in 1996 to describe these operations instead of information warfare which now has a specific meaning.

This thesis is unclassified and discusses only unclassified information. All definitions, conclusions, and recommendations are based upon unclassified, open source documents. All definitions used come from either of two unclassified sources: JOINT CHIEFS OF STAFF, PUBLICATION 3-13 JOINT DOCTRINE FOR INFORMATION OPERATIONS (21 January 1997) (Draft) [hereinafter JCS PUB. 3-13] or DEP'T OF ARMY, FIELD MANUAL 100-6, INFORMATION OPERATIONS (1996) [hereinafter FM 100-6]. Although there are two primary documents classified at the classified secret level which provide the working definitions in this area, due the unclassified nature of this thesis, the definitions in JCS Pub. 3-13 and FM 100-6 will be used. *See generally* DoD Directive (S) 3600.1, Information Operations, 9 December 1996, and CHAIRMAN, JOINT CHIEFS OF STAFF, INST. (S) 3210.01 INFORMATION WARFARE (2 January 1996) [hereinafter CJCSI 3210.01]. It should be noted here that CJCS MOP 30, Command and Control Warfare is superceded by CJCSI 3210.01. *See* CHAIRMAN, JOINT CHIEFS OF STAFF, NOTICE 3205, CANCELLATION OF CJCS MOP 30 (September 30, 1996) *canceling* CHAIRMAN, JOINT CHIEFS OF STAFF, MEMORANDUM OF POLICY, NO. 30., COMMAND AND CONTROL WARFARE, (July 17, 1990; March 8, 1993).

present.[5] It is critical that we quickly grasp and understand the scope and impact of information operations and information warfare in order to confront and control the information challenges of the 21st Century.

---

[5] A complete list of such reading material would be enormous, however, as of list date, several important publications, many of which will be discussed and relied upon in this thesis, include: JOINT CHIEFS OF STAFF, INFORMATION WARFARE: A STRATEGY FOR PEACE . . . THE DECISIVE EDGE IN WAR 1 (1996) [hereinafter A STRATEGY]; JOINT CHIEFS OF STAFF, JOINT VISION 2010 16 (1996) [hereinafter JOINT VISION]; JCS PUB. 3-13, *supra* note 5; DEP'T OF THE AIR FORCE, A PRIMER ON LEGAL ISSUES IN INFORMATION WARFARE (1995) [hereinafter PRIMER]; FM 100-6, *supra* note 5; GOV'T ACCOUNTING OFFICE, REPORT, INFORMATION SUPERHIGHWAY - AN OVERVIEW OF TECHNOLOGY CHALLENGES, B-259205, GAO/AMID-95-23 January 23, 1995; CYBERWAR: SECURITY, STRATEGY, AND CONFLICT IN THE INFORMATION AGE (Alan D. Campen, et al. eds, 1996); ALAN D. CAMPEN, THE FIRST INFORMATION WAR: THE STORY OF COMMUNICATION, COMPUTERS, AND INTELLIGENCE SYSTEMS IN THE PERSIAN GULF (Alan D. Campen, ed., 1992); MARTIN C. LIBICKI, NAT'L DEF. U., WHAT IS INFORMATION WARFARE? (1995) [hereinafter LIBICKI]; ROGER C. MOLANDER ET AL., STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR (1996) [hereinafter MOLANDER]; ANDREW H. NELSON, THE ART OF INFORMATION WAR (1995); ALVIN TOFFLER AND HEIDI TOFFLER, WAR AND ANTI-WAR: SURVIVAL AT THE DAWN OF THE 21ST CENTURY (1993) [hereinafter TOFFLERS]; SCHWARTAU, *supra* note 4; Ralph J. Andreotta, *The National Information Infrastructure: Its Implications, Opportunities, and Challenges,* 30 WAKE FOREST L. REV. 221 (1995); M. E. "Spike" Bowman, *Essay: Is International Law Ready for the Information Age?,* 19 FORDHAM INT'L L.J. 1935 (1996) [hereinafter Bowman]; Sean P. Kanuck, *Recent Development: Information Warfare: New Challenges for Public International Law,* 37 HARV. INT'L L.J. 272 (1996) [hereinafter Kanuck]; Richard A. Morgan, *Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and "Peaceful Purposes,"* 60 J. AIR L. & COM. 237 (1994) [hereinafter Morgan]; Henry H. Perritt, Jr., *Access To The National Information Infrastructure,* 30 WAKE FOREST L. REV. 51 (1995); John I. Alger, *Declaring Information War,* JANE'S INT'L DEF. REV., Jul. 1996, at 54; Gary H. Anthes, *DoD On Red Alert to Fend Off Info Attack,* COMPUTERWORLD, Jan. 6, 1997, at 1; Gary H. Anthes, *New Laws Sought For Info Warfare,* COMPUTERWORLD, Jun. 5, 1995, at 55 [hereinafter New Laws]; John Arquilla & David Ronfeldt, *Cyberwar is Coming!,* COMPARATIVE STRATEGY, Apr.-Jun. 1993, at 24 [hereinafter Arquilla]; Andrew C. Braunberg, *Air Force Pursues Two-Sided Information Warfare Strategy,* SIGNAL, Jul. 1996, at 63 [hereinafter Braunberg]; Alan D. Campen, *Assessments Necessary in Coming To Terms With Information War,* SIGNAL, Jun. 1996, at 47. More material is produced everyday as newer technology is developed and employed. As this area experiences change so quickly because of technological advances, terminology becomes outdated rapidly.

Despite assertions that the Information Age raises many legal issues without clear precedent,[6] this thesis argues that the current international law paradigm can be applied effectively to information operations and information warfare. This is best accomplished by employing an incrementalist view of international law. In a swiftly changing environment such as the Information Age, the incrementalist approach pursues incremental, evolutionary changes and revisions of a current framework in order to adapt to the changes in the environment. It does not view it as necessary to establish a completely new framework of analysis for changes in the environment. Additionally, employing the "net effect" principle, which works within the current paradigm and focuses upon the intent and result of an operation, it will be possible to determine the legality of information operations. This thesis will discuss information operations, as well as the current international law applicable to information operations. It will present a workable legal framework applicable to information operations, and apply this framework to several scenarios employing information operations. This application process will demonstrate that the incrementalist approach, combined with the net effect principle, is the proper approach to undertake to analyze current information operations.

Some writers argue that information-based technological advances have caused a "revolution in military affairs" which is radically transforming warfare into the warfare of the

---

[6] RICHARD W. ALDRICH, INSTITUTE FOR NATIONAL SECURITY STUDIES, THE INTERNATIONAL LEGAL IMPLICATIONS OF INFORMATION WARFARE, INSS OCCASIONAL PAPER 9 (April 1996) [hereinafter ALDRICH]; PRIMER , *supra* note 6; Kanuck, *supra* note 6.

"third wave."[7] Such a revolutionary process would require the development of new legal paradigm.[8] Other writers, however, assert that the advancements in information technology

---

[7] ALVIN TOFFLER AND HEIDI TOFFLER, WAR AND ANTI-WAR: SURVIVAL AT THE DAWN OF THE 21ST CENTURY (1993). The Tofflers argue that human society has gone through three "waves," with each wave based on the means in which wealth was created. The first wave was the agrarian, the second the industrial, and now we are in the third wave which is the information wave. Some writers disagree with the Tofflers' theory. *See e.g.*, R. L. DiNardo & Daniel J. Hughes, *Some Cautionary Thoughts on Information Warfare*, AIRPOWER J., Winter 1995, at 69 ("The Tofflers' book, although not widely reviewed in the scholarly literature, has received tremendous attention and acclaim within the government, gaining the approbation of people as influential as the Speaker of the House of Representatives. The Tofflers have been most successful in getting the military, especially the Army and the Air Force, to accept the basic premise of their "wave" theory . . . . Although the Army is somewhat more skeptical of the Tofflers' notions, the wave theory essentially was adopted officially in *Army Focus 94: Force XXI* . . . . The very simplicity of the Tofflers' theory makes the book highly attractive. However, *War and Anti-War* is a book full of mistakes. Any historian seeking to bring out these errors would find *War and Anti*-War, to use an Air Force term, a *target–rich environment.* revolution."); *Misinformed About Information War? The Three-Wave Theory Is Under Fire*, DEF., & FOREIGN AFF. STRATEGIC POL'Y, Mar. 1986, at 4 ("The Tofflers are no military historians and it shows in their definitions here in their three ages."); Robert J. Bunker, *Generations, Waves, and Epochs: Modes of Warfare and the RPMA*, AIRPOWER J., Spring 1996, at 18 ("As I have stated, the Tofflers have promoted the most popularized theory of future war. Components of their third-wave war theory, however, may be critically flawed. For that reason, it should be compared to the other two theories highlighted in this essay before it is acknowledged as *the* authoritative work on this subject."). Robert J. Bunker, *The Tofflerian Paradox*, MIL. REV., (May-Jun. 1995) at 99 ("The war forms developed in *War and Anti-War*, specifically First and Second Wave war, are overgeneralized and distort Western warfare's historical development."); Thomas J. Czerwinski, *The Third Wave: What the Tofflers Never Told You*, STRATEGIC F., Apr. 1996, No. 72 (discussing the point that the Tofflers' analysis is incomplete in that it does not reflect the specific conditions existing in the Third Wave which make it a revolution in military affairs. Czerwinski argues that the Information Age is only one of the components of the Third Wave.).

[8] *Hearing on Revolutions in Military Affairs Before the Senate Armed Services Comm. Subcomm. on Acquisitions and Technology*, 103rd Cong. (May 5, 1995) (statement Andrew W. Marshall, Director, Net Assessment, Office of the Secretary of Defense) ("The Office of Net Assessment and others are investigating the hypothesis that over the next 20 to 50 years a military revolution will transform the ways wars are fought . . . . There are two major ideas about how warfare may change . . . . The first is that 'long-range precision strike weapons coupled to very effective sensors and command and control systems will come to dominate much warfare. Rather than closing with an opponent, the major mode will be destroying him at a distance.' The second aspect of the emergence of 'information warfare,' Mr. Marshall

said. 'Much as over the last sixty to seventy years one wishes to obtain air superiority in order to better conduct all other military operations, in the future, obtaining early superiority in the information area may become central to doing well in warfare.'"). *See generally* Captain James H. Patton, *The New "RMA": It's Only Just Begun,"* NAVAL WAR COLLEGE REV., Spring 1996, at 23; MICHAEL L. BROWN, *The Revolution in Military Affairs: The Information Dimension, in* CYBERWAR: SECURITY, STRATEGY, AND CONFLICT IN THE INFORMATION AGE, 31 (Alan D. Campen, et al. eds, 1996); Colonel Richard F. Riccardelli, *The Information and Intelligence Revolution,* MILITARY REV., Sept.-Oct. 1995, at 82. *See also* John T. Correll, *Signs of a Revolution,* AIR FORCE MAG., Aug. 1995, at 2 ("Over the years, there have been periodic innovations leading to wholesale changes in the ways that wars were fought. Generally accorded to have been among these developments were the longbow, the cannon, the airplane, and the ballistic missile. In a few instances, change was immediate. From the moment the atomic bomb was introduced in 1945, all nonnuclear warfare has automatically been regarded as 'limited war.' Most changes took effect gradually, though. The rifle was in everyday use for more than a hundred years as a sporting arm before it replaced the musket as the standard military shoulder weapon. The popular term for such a change, a 'Revolution in Military Affairs,' was invented in 1982 by Marshall N. V. Ogarkov of the Soviet General Staff, who held that the precision and effectiveness of advanced conventional weapons represented a benchmark in the history of warfare. Marshal Ogarkov's term has been borrowed and broadened by Western theorists to describe a basic shift they believe to be under way . . . ."); Major Norman C. Davis, *An Information-Based Revolution in Military Affairs,* STRATEGIC REV., Winter 1996, at 43 ("The Information Revolution is a product of advances in computerized information and telecommunications technologies and related innovations."); Lieutenant Commander Randall G. Bowdish, *The Revolution in Military Affairs: The Sixth Generation,* MIL. REV., Nov. - Dec. 1995, at 26 ("Military history is full of examples of nations searching for methods and weapons to provide a decisive edge in warfare. Remarkably, despite many technological advances made throughout history, very few have resulted in the decisive edge envisioned"); James R. Fitzsimmonds & Jan M. van Tol, *Revolutions in Military Affairs,* JOINT FORCE QUARTERLY, Spring 1994, at 24-31 ("The full RMA realization must have three preconditions: technological development, doctrinal innovation, and organizational adaptation."); STEVEN METZ & JAMES KIEVIT, STRATEGY AND THE REVOLUTION IN MILITARY AFFAIRS: FROM THEORY TO POLICY, unpublished manuscript on file with the Strategic Studies Inst., U.S. Army War College, Carlisle Barracks, P.A. (1995) ("A small band of "RMA" analysts has emerged in the military and Department of Defense, in the academic strategic studies community, and in defense-related think-tanks and consulting firms. To these analysts, the Gulf War provided a vision of a potential revolution in military affairs (RMA) in which 'Information Age' technology would be combined with appropriate doctrine and training to allow a small but very advanced U.S. military to protect national interests with unprecedented efficiency.").

are causing only gradual, evolutionary changes affecting various aspects of society, particularly in military operations.[9] Although these same information-based technological advancements are capable of completely shutting down modern economies and any armed forces that threaten United States' interests, I assert that these changes in warfare technology are incremental in nature, in light of the overall nature of conflict among nations, and do not warrant a complete revision of the existing legal framework.

---

[9] COLONEL RICHARD J. DUNN III, NAT'L DEF. U., FROM GETTYSBURG TO THE GULF AND BEYOND: COPING WITH REVOLUTIONARY TECHNOLOGICAL CHANGE AND LAND WARFARE (1996) (The primary goal of his analysis is to discern our ability to understand the distinction between "evolutionary" and "revolutionary" change and "To comprehend the total impact of technology on warfare."); Lieutenant Colonel Thomas X. Hammes, *The Evolution of War: The Fourth Generation,* MARINE CORPS GAZETTE, Sept. 1994, at 35 (discusses the premise argued by author William S. Lind in 1989 regarding the generations of warfare and develops the concepts about the fourth generation of warfare.); William S. Lind et al., *The Changing Face of War in to the Fourth Generation,* MIL. REV., October 1989, at 2 (The authors look at the makeup of war in recent generations and posit that we are on the verge of a new generation. They see this generation as one that may combine very different methods of waging war with significant new technology. The fourth generation will see an expansion of the battlefield to include the whole of the enemy's society; decreasing dependence on centralized logistics; more emphasis on maneuver – small, highly maneuverable, agile forces will tend to dominate; and the goal of collapsing the enemy internally rather than physically destroying him. "In broad terms, fourth-generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred tot he vanishing point. It will be nonlinear, possibly to the point of having no definable battle lines or fronts; the distinction between civilian and military may disappear; actions will occur concurrently throughout all participants' depth, including their society as a cultural, not just a physical entity."); *Winning the Information War: Evolution and Revolution,* speech delivered by General Frederick M. Franks, Jr., at the Association of the U.S. Army Symposium, Orlando, Florida, Feb. 8, 1994, in VITAL SPEECHES, May 15, 1994, at 453 ("You may never know when you are in a transition period. Later, when you look back with a historical perspective it becomes clearer. Well, I believe we are in one of those now. I think we can all say that with some certainty. We evolved into it as we saw the information age dawn in Desert Storm. A lot of the old continued – back to the reality of land combat and a lot of the new emerged also. A glimpse of the future, if you will. There we saw some glimmerings of the dawn of a new era in land warfare. Some evolutionary changes and perhaps some revolutionary changes as well.").

It appears that contemporary society is having some difficulty in applying many current principles and analytical models to information warfare/operations.[10] At first glance, information operations, particularly those involving computers and computer systems, appear to be a completely new phenomenon. However, after analysis, most information operations fit within the contemporary framework of analysis. For example, the concept of attacking an opponent with a computer in cyberworld through the Internet initially appears to be completely outside the realm of any current physical framework of analysis. But when one focuses upon penetrating the traditional issues of the identity of the actor and the effect of the action, rather than concentrating solely upon the computer-based nature of the action, one moves to a level of analysis centering upon the intent and net effect of the act. This allows

---

[10] James Adams, *Crooks Face CIA Hackers,* SUNDAY TIMES, October 27, 1996, *available in* LEXIS, News Library, Txtnws File ("The CIA is going into cyberspace to attack a new generation of criminals with computer viruses. President Bill Clinton is expected to approve a range of covert actions designed to take the campaign to stop criminals into the most sophisticated technological realms. The measures will allow the CIA and the National Security Agency (NSA) to hack into the records of bank accounts held by known international terrorists and steal their money. They will also enable the agencies to plant bugs and viruses inside the computers used by terrorists and their sponsors. Since the end of the Cold War, a new breed of computer-literate terrorist and organized criminal has emerged. Every terrorist organization has an array of personal computers and drug barons investing millions of dollars each year to upgrade computer systems that keep track of their operations."); *New Laws, supra* note 6 ("We need a comprehensive legal framework to protect information systems," said Admiral William O. Studeman, deputy director of the CIA, in a recent speech. "[We need] hacker prosecution laws, [a] better definition of computer crime and an examination of the legal basis for [an] appropriate government role in protecting information systems.") *See also* Richard Behar, *Who's Reading Your E-Mail? As the World Gets Networked, Spies, Rogue Employees, and Bored Teens Are Invading Companies' Computers to Make Mischief, Steal Trade Secrets -- Even Sabotage Careers,* FORTUNE, February 3, 1997, at 56 ("Speaking before hundreds of computer experts from IBM, Fidelity Investments, Mobil, the Secret Service, U.S. Customs, and other institutions last fall, Dennis Hughes, the FBI's senior expert on computer crime, declared flatly: 'The hackers are driving us nuts. Everyone is getting hacked into. It's out of control.' In October 1996, President Clinton signed into law a new bill that should make it easier to prosecute hackers. The bill allows for criminal forfeiture, fines of $10 million, and sentences of 15

one to uncover the essential facts to which contemporary models may be applied. Is there a difference between a nation dropping conventional iron bombs on another country and "dropping" computer logic bombs into another country's infrastructure? Are they both considered acts of aggression or uses of force? These questions will be explored later in this thesis, however; it is important to realize that the essential nature of conflict and war remains unchanged, although their "character is now in constant transition."[11]

Information has played an important role in success on the battlefield throughout history.[12] A Chinese general, Sun Tzu, who lived in the 4th century BC wrote one of the

---

years in computer cases involving economic espionage – broadly defined as stealing trade secrets form U.S. companies.").

[11] A STRATEGY, *supra* note 6, at 1.

[12] *See generally* MICHAEL HANDLE, SUN TZU & CLAUSEWITZ COMPARED, 40-60 (1991) (compares the two most highly regarded classic texts on warfare. The section on deception, surprise, intelligence, and command and control speaks to issues related to information warfare. The authors tries to reconcile the two grand masters of strategy, however, Handle finds some real differences in areas of special interest to information-based warfare, such as: deception, surprise, intelligence, and command and control. For example, on command and control in battle, Sun Tzu writes that it is "difficult but possible," while Clausewitz believes it is "very difficult if not impossible."). CARL VON CLAUSEWITZ, ON WAR (Michael Howard & Peter Paret, eds. & trans. 1983) ("War is not an independent phenomenon, but the continuation of politics by different means. Consequently, the main lines of every major strategic plan are largely political in nature, and their political character increases the more the plan applies to the entire campaign and to the whole state. A war plan results directly from the political conditions of the two warring states, as well as from their relations to third powers.") Id. at 8 citing C. v. Clausewitz to C. v. Roeder, 22 December 1827, in *Zwei Briefe des Generals von Clausewitz*, special issue of the *Militarwissenschaftliche Rundschau*, 2 (March 1937). SUN TZU, THE ART OF WAR (Samuel B. Griffith, trans. 1971) (hereinafter ART OF WAR) (this ancient text on warfare is popular due to Sun Tzu's holistic view of warfare and the increasing irrelevance of Clausewitz's classic *On War* in the Information Age. Unlike Clausewitz, Sun Tzu regards information as indispensable in reducing the uncertainty of war. Much of *The Art of War* is arguably applicable to information warfare.). Lieutenant Colonel Anthony M. Coroalles, *On War in the Information Age: A Conversation with Carl von Clausewitz*, ARMY, May 1996, at 24 (in a mock interview between the author and Clausewitz regarding the information age, Clausewitz says that "[m]y point is that even

oldest and most respected treatises on the subject of war: *The Art of War*. Sun Tzu said that the greatest achievement of a commander was to destroy the enemy's strategy before it could be implemented.[13] Sun Tzu professed that "[t]o subdue the enemy without fighting is the acme of skill."[14] As such, information warfare or "Sun Tzu Style" warfare[15] includes not

---

though the means of waging war have changed greatly from my day, the nature of war remains fundamentally unchanged. War continues to be an act of violence guided by political aims in which human intelligence, will, and emotion compete freely. . . . As I observe your modern society, I see another center of gravity emerging – information. Every component of your national power depends on the free flow of information and the maintenance of information-based systems. Your military, economy, communications, media, educational system, financial system and transportation system are fueled by information. Information is the central feature of your power and, unlike previous times, it is a feature that your military may not be able to protect from attack. An opponent can directly attack this vital element without first defeating your military. In my opinion, it is an uncovered and unprotected source of great power and is perhaps also your greatest vulnerability. . . . Remember that war is a human phenomenon, and as such, it is subject to all the forces that make human interaction so unpredictable. War is chaotic, and attempts to control chaos are, by definition, doomed to fail. What you must strive to do is develop soldiers, systems, and organizations to operate in that chaos and uncertainty. If you can do that, I believe that you will be able to meet whatever challenges war in the information age brings.").

[13] *A Survey of Defence Technology*, THE ECONOMIST, Jun. 10, 1995, at 5 ("This had to be done in an unexpected way, with the unconventional use of 'divine force,' *ch'i*. The opposite of *ch'i* was the ordinary force, *cheng*. On the battlefield, *cheng* is a holding force that puts the enemy on the spot, *ch'i* a flanking maneuver that fatally disrupts the enemy's strategy. This is how Genghis Khan fought, and also how Norman Schwarzkopf fought. It is now possible that information could take the place of *cheng*. Imagine two chess players, both with good memories, both blindfolded; and adjudicator tells them when their pieces are in a position to make a capture. This game, called *Kriegspiel*, was used to teach caution in Prussian was colleges. Though its rules are those of chess, its tactics are not; they are cautious and edgy. Now imagine one of the players taking off the blindfold. He can throw caution to the winds, and dispatch his adversary in instants with only a fraction of his available force. They enemy would be paralyzed not by an opposing ordinary force, but by his own ignorance – frozen in the headlights that illuminate his every move. The response is obvious: blind your opponent.").

[14] ART OF WAR, *supra* note 14, at 22.

[15] I created this term because I believe that contemporary technological advances in information systems allow us greater capability to employ our military more effectively, even more lethally in some situations, than relying primarily on brute force.

only elements from conventional warfare – deception and misinformation[16] – but also the newer information-based system techniques such as computer intrusion and disruption, data manipulation, and telecommunications spoofing.[17]

The concept of warfare waged from a keyboard fosters the development of a misleading notion that future conflict will be bloodless.[18] It envisions a very futuristic type of battle occurring somewhere in "cyberspace."[19] Out in cyberspace US "information

---

[16] During the process of developing and updating doctrine and policy materials on information warfare , DoD decided to substitute the term "information operations" for "information warfare" due to the negative implications connected with the term "warfare." The term information warfare now only refers to information operations during times of crisis, conflict, and war. Interview with Colonel John Burton, Legal Counsel, Chairman's Legal Counsel Office, in Pentagon, Washington, D.C. (Jan. 11, 1997).

[17] "Packet spoofers" disguise their senders or impersonate other users to potentially sow dissemination." Peter Costantini, *Technology-Information: Could Cyberwars Be Another Pearl Harbor?*, INTER PRESS SERV., Aug. 9, 1996, *available in* 1996 WL 10768645. Interview with Mr. Allen Keener, Information Operations Contractor Support, Dep't Army, Office of the Deputy Chief of Staff for Operations and Plans, Information Operations Division, in Pentagon, Washington, D.C. (Jan. 21, 1997) (it is difficult to track all computer intruders due to their ability to disguise themselves to avoid detection). *See also* FM 100-6, *supra* note 5.

[18] Carl von Clausewitz believed that the idea of nonlethal weapons was a dangerous concept. He stated: "Let us no hear of Generals who conquer without bloodshed. If a bloody slaughter is a horrible sight, then that is a ground for paying more respect to War, but not for making the sword we wear blunter and blunter by degrees and feelings of humanity, until some one steps in with one that is sharp and lops off the arm from our body." CARL VON CLAUSEWITZ, ON WAR 345 (Anatol Rapoport ed., 1968). During the Battle of Fredricksburg, General Robert E. Lee said that "[i]t is well war is so terrible, or we should grow too fond of it." DOUGLAS SOUTHALL FREEMAN, R. E. LEE: A BIOGRAPHY, Vol. 2 462 (1941).

[19] EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW: YOUR RIGHTS AND DUTIES IN THE ON-LINE WORLD 1 (1994) (interaction in the non-physical universe known as "cyberspace" is mediated by computers linked over the telephone network. Science fiction author William Gibson is credited with coining the term in his novel NEUROMANCER. "Gibson's concept included a direct brain-computer link that gave the user the illusion of physically moving about in the data 'matrix' to obtain information. In Gibson's vision, cyberspace is a 'consensual hallucination that felt and looked like physical space but actually

was a computer-generated construct representing abstract data."); Lawrence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier,* THE HUMANIST, March 26, 1991, at 15 ("As commonly used today, cyberspace is the conceptual 'location' of the electronic interactivity available using one's computer. Cyberspace is a place 'without physical walls or even physical dimensions' in which interaction occurs as if it happened in the real world and in real time, but constitutes only a 'virtual reality.'"); HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING THE ELECTRONIC FRONTIER 5 (1993) ("Cyberspace is the manifestation of the 'words, human relationships, data, wealth, and power . . . by people using $ (computer-mediated communications)."); *See generally* FLEMING JAMES, JR., ET AL., CIVIL PROCEDURE § 2.4 – 2.8 (1992) ("Activity in cyberspace, however, creates new relationships among individuals that differ form their analogues in the more usual, physical existence. These new relationships strain legal principles and categories that currently direct judicial power over individual action, either civilly or criminally. The fundamental jurisdictional premise of the common law is physical presence, either actual or constructive, within the jurisdiction attempting to assert authority over an individual. The body of the individual may be located in the jurisdiction, the individual may perform an action that has physical effects within the jurisdiction, or the individual may transfer some physical object into the jurisdiction. In addition, the boundaries of the jurisdiction itself are defined in physical, geographical terms. In a very relevant sense, cyberspace is a new, and separate, jurisdiction. Of course, it cannot exist independently of the real world, which is organized into its geographical jurisdictions, and the inhabitants of cyberspace are also citizens of a physical jurisdiction."). *See also* William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community,* 30 WAKE FOREST L. REV. 197 (1995) (arguing that current domestic legal principles are wholly inadequate to deal with cyberspace interaction. Rather, Byassee calls for recognition of and sensitivity to the differences of cyberspace, and promotes legislative action rather than judicial distortion of existing statutes simply because of judicial disapproval of the conduct observed.). *See also For CIA, "Cyber" Doesn't Compute,* USA TODAY, Jul. 17, 1996, at A2 ("CIA Director John Deutch was a witness at Senate hearings in June 1996 on the United States' vulnerabilities to information terrorism. Deutch left one question, posed by Sen. Sam Nunn, D-Ga., unanswered. In a rare display of the CIA's lighter side, Deutch followed up with this letter: Dear Senator Nunn: During yesterday's hearing on foreign information warfare capabilities you asked a rather indelicate question: 'What does 'cyber' mean, anyway?' I must admit that your query caused a great deal of discomfort here. While everyone had used the term, no one had heretofore felt any need to know precisely what it meant. In light of my promise to keep Congress fully and currently informed, I pressed for an answer. Central Intelligence Agency's (CIA) research revealed that the term 'cybernetics' was coined by the Father of Cybernetics, Norbert Wiener, in 1948. In Mr. Wiener's words, 'We have decided to call the entire field of control and communication theory, whether in the machine or the animal, by the name cybernetics, which we form from the Greek kybernetes or 'steersman.' Department of State concurred with CIA's findings, but wished to point out that the Greek kybernetes is related to the Latin gubernator, meaning 'steersman' or 'governor.' The Defense Intelligence Agency is not yet ready to make a judgment, and is exploring the possibility that 'cyber' may have come from the Greek kybisteter or 'diver,' from which we also derive the word 'cybister' or 'a genus of large

warriors" would be capable of disabling important enemy military or civilian vital infrastructure systems with little, if any, loss of life.[20] Nevertheless, it is very easy to develop such perceptions now when our knowledge of information operations or information warfare is limited by our current imperfect knowledge of its immensity.

---

diving beetles.' I hope this clears up any confusion. Sincerely, John Deutch, Director of Central Intelligence.").

[20] Douglas Waller, *Onward Cyber Soldiers: The U.S. May Soon Wage War by Mouse, Keyboard and Computer Virus, But It Is vulnerable to the Same Attacks*, TIME, Aug. 21, 1995, at 38 (hereinafter Waller). Others have commented that war in the future will only use the information warrior to enhance the blood battle. *See, e.g.*, Charles Dunlap, *The High-Tech War of 2007*, THE WEEKLY STANDARD, Jan. 29, 1996, at 22 (discussing traps we may easily fall into if we are not cautious concerning information technology. Some of these traps include: an increasing reliance upon commercial, off-the-shelf cybertechnology; advances in computer software eroding the demand for highly trained specialists to penetrate complex weapons; easy to learn graphic displays which allow poorly educated soldiers to quickly master elaborate and complex but user-friendly war-fighting machines, rather like a 15-year-old American figuring out how to dispense Coca-Cola at a fast-food restaurant by pressing the right pictograph; the microchip ending the educational and training advantage the American military has enjoyed; believing that information technologies reduce the need for conventional combat forces, and thus disbanding such conventional forces in favor of trendy "information" units which will be filled not with well-trained, physically fit combatants, but rather, "mind-nimble (not necessarily literate), fingertip-quick youth" who tend to equate their success at video games with competency to engage in real war. The technology-spurred globalization of the news industry will become a means of making war. International news organizations using the latest electronic wizardry will no longer have to depend on government held press conferences in war zones. Operational security will become impossible as news groups launch their own information-gathering and communications satellites; monitor proliferating Internet transmissions; give their reporters self-contained communications suites; and, even fly their own unmanned aerial reconnaissance vehicles to transmit real-time views of battle areas. This information also will be available to the enemy who then has no need to build costly satellites or even pay spies; instead they can rely on the free flow of data. The technology-empowered media make "information equality," not "information dominance," the key to the "revolution in military affairs.").

There is an updated Indian fable which tells how seven mice eventually discover an elephant. This story provides a helpful analogy which we can apply to information operations. The fable begins with the seven mice exploring a large object:

> The first, arms encircling its leg, thought he was feeling a pillar.
> The second, contending with its writhing trunk, thought it like a snake.
> The third, encountering its pointy tusk, "saw" a spear.
> The fourth, assessing its massive flank, disputed his sightless comrades, insisting that the elephant was like a great cliff.
> The fifth, grasping the ear, proclaimed the elephant was a fan.
> And the sixth, grasping its slender tail, perceived the elephant as very much like a rope.
> They could not agree on what it was until the seventh went to explore.
> The seventh, ran up one side and down the other and across the top from one end to the other.
> After considering what the others had experienced, the seventh one proclaimed it an elephant.
> The moral: knowing in part may make a fine tale, but wisdom comes from seeing the whole.[21]

Right now, we are like the mice searching out and gaining knowledge of the various parts of the elephant. We know bits and pieces about the "thing" before us and have developed partial knowledge or perceptions about what it is. However, we have not gathered

---

[21] ED YOUNG, SEVEN BLIND MICE (1992). SEVEN BLIND MICE retells the Indian fable "Blind Men and the Elephant." The original Indian tale portrays seven blind men rather than blind mice discovering different parts of an elephant and arguing about what it is that is before them. I remembered this childhood story when Lieutenant Colonel Elizabeth Anderson, Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence, Information Warfare, presented it during her briefing on "Information Operations" on March 4, 1997, at the Intermediate Information Warfare Course, School of Information Warfare Strategy, National Defense University, Ft. McNair, Washington, D.C. I believe that this fable perfectly synthesizes the essence of my thesis. I argue that we, like the blind mice, have insufficient knowledge of the entire spectrum of capabilities and vulnerabilities of information operations at this time to be able to declare with definitiveness what is information operations or to posit a new international legal paradigm. Like the seventh mouse, we will arrive at our answer based upon the experiences and information gathered over time as we proceed through the Information Age.

and processed all the information to enable us to comprehend the entire "thing."[22] At this period in the Information Age, we have not acquired enough data to comprehend completely what it is that we are actually calling information operations. Clearly, we know something is out there that we have recently labeled "information operations," however, our "knowledge" is still in an imperfect state. Under these circumstances, the incrementalist approach is the best method to use to distill the working body of law applicable to information operations. It allows us to continue to gather and process information and apply the law to it.

---

[22] It appears now that the rapidly changing nature of information-based technology may be confounding and overwhelming the general public. *See e.g.*, Lou Dolinar, *It's Not Easy to Get the Elephant to Balance the Ball*, THE DAILY PROGRESS, May 2, 1997, at 15 ("So there are these three visually challenged yuppies at the zoo, checking out their first elephant. Whaddaya think guys? Meanwhile, the elephant has playfully entwined its trunk around the third yuppie. 'Way cool,' he says. 'Reminds me of that snake thing that's no in the movies . . . " Then the elephant sits down and crushes them That's the Internet, gang. It's big; it's different things to different people, and it has decided to sit down right smack dab in the middle of our lives."); Jennifer Tanaka, *Drowning in Data: Feeling Overwhelmed by Information? It's Time to Get Rid of Some Gadgets*, NEWSWEEK, Apr. 28, 1997, at 85 (David Shenk's book, DATA SMOG (1997) discusses that "today's abundance of information, while generally good for society, is having some bad unintended side effects on individuals. The excess, Shenk writes, has created a noxious environment of overstimulation that's pushing people to their limits. Psychologists are seeing more and more cases of stress caused by 'information overload.'"). *Cf.*, David McCracken, *A New Generation Powers Up: As Mentors and Pen Pals, the Young At Heart Are Signing on in Big Numbers*, CONNECT-TIME, May 1997, Vol. 1, Issue 7, at 6 ("A national survey conducted recently for SeniorNet by Frederick/Schneiders marketers discovered that computer ownership among adults aged 55 to 75 is at 30 percent and growing fast."); Joe Mullich, *Self-Health: Embracing the Online World of Second Opinions*, CONNECT-TIME, Apr. 1997, Vol. 1, Issue 6, at 8 ("Hundreds of thousands of people are going online to investigate medical options they haven't found through traditional channels, arming and empowering themselves with the kind of knowledge essential for sound decisions about their own health. Some of these are the life-and-death stories that wind up in the local newspaper. But many are not. Every facet of health care in America is being shaped by online access, from prescription facts to experimental treatments for rare diseases. The Internet has the potential to become, in time, the ultimate self-help resource.").

The incrementalist approach focuses upon the continuous incremental change and revision within a current framework, rather than automatically pursuing wholesale change. [23] A maximalist approach calls for a new paradigm and quickly "throws the baby out with the bath water" while arguing that current regime is no longer applicable, while a minimalist approach seeks a distillation of the existing principles or paradigm. [24] The radical approaches are best advocated when the "whole" is known and understood. Therefore, only when one knows the "whole" could he or she argue that the "whole" as known does not fit a certain paradigm.[25] The incrementalist approach is most appropriate when uncertainty exists,

---

[23] The terms incrementalist, maximalist, and minimalist are defined and discussed in THE PRINCIPLES OF WAR IN THE 21ST CENTURY: STRATEGIC CONSIDERATIONS. The authors discuss their approach to the revision of the principles of war for the 21st Century, and they assert that their recommendation "for revising the principles of war are not radical." They argue that their changes are incremental, in the nature of small change, updating, rather than wholesale change. They contend that they were able to do this because the principles of war, as they exist, have been so carefully honed over time that they reflect "truth" as accurately as possible. They submit that there are two radical alternatives immediately come to mind. "One might be called the "maximalist" approach, which posits that war has become so complex that no single set of principles can apply to all of war's variations. The time tested principles work for conventional combined arms warfare, but a totally different set of principles would be required for guerrilla warfare, *information warfare*, or other forms. At the other extreme, the "minimalist" approach suggests that the existing principles of war can be further distilled (emphasis added)." William T. Johnson, et al., *The Principles of War in the 21st Century: Strategic Considerations*, Aug. 1, 1995, unpublished manuscript on file with the Strategic Studies Inst., U.S. Army War College, Carlisle Barracks, P.A. (1994), at 4. These same terms and concepts will be used in this thesis to discuss the international law paradigm applicable to information warfare.

[24] *See* Kanuck, *supra* note 6. This article argues that the current international law paradigm is no longer feasible. The writer, however, does not provide a suggested paradigm to replace the current one.

[25] The reason Mr. Kanuck is unable to suggest a new paradigm is because we do not have complete knowledge of information operations at this time to even try to develop another paradigm or legal structure. All Mr. Kanuck argues is that information operations are somehow different; but there is no earnest attempt to try to work with such operations within the current framework. It is much easier to point out their newness and that they appear not

particularly because of the magnitude of an enigmatic issue such as information operations. In essence, we must wait to see if it is an elephant, a rhinoceros, or a fictitious wookie before we label it and assign it a new category.[26]

This thesis addresses the challenges information operations present and argues that our current international legal framework regarding armed conflict is responsive to our needs at this time. Section II will discuss briefly the nature of the information age and the development of information warfare and operations.[27] Section III will focus on an incrementalist application of international law to information operations conducted during periods of peace, crisis, and conflict. It will also discuss the nature of the "net effect" principle in the application of an international law analysis. This section IV will provide a useful international law analysis framework for attorneys encountering information operations. This will be followed by using the framework and applying the incrementalist approach and the net effect principle to several hypothetical fact patterns. Based upon the framework and analysis it produces, it is clear that that the current legal paradigm is applicable to information operations.

---

to fit within current mechanism, rather than to show that it is impossible to analyze these operations within the current mechanisms.

[26] A wookie is a large, hairy, futuristic hybrid creature in the motion picture STAR WARS (20TH Century Fox 1978).

[27] Dr. Fredrick Giessler a Professor at the School of Information Warfare Strategy of the National Defense University, Ft. McNair, Washington, D.C., commented during the Intermediate Information Warfare Course, School of Information Warfare Strategy, National Defense University, Ft. McNair, Washington, D.C., that trying to pin down a definition or concept in information operations is "like taking a picture of an fast moving object – all you get is a blur" (Mar. 3, 1997).

II. The Information Age and Information Operations

The concept of the Information Age is characterized by the acceleration in the growth of information, information source, and information dissemination capabilities supported by information technology. There has been an explosion in the development of the technical means of collecting, storing, analyzing, and transmitting information. Information systems technologies include such elements as telecommunications, automated data processing, sophisticated decision aids, remote sensors, and other related systems.[28] "The spectrum of applied technologies ranges from established radio frequency, microwave, satellite, coaxial, and fiber optic transmission systems to new generations of digital and advanced personal communications systems."[29] Consequently, these information technologies swiftly concentrate data, vastly increase the rate at which we process it, and inextricably combine the results into virtually every aspect of our lives. By being able to provide military commanders with information in such unprecedented quantity, quality, and accuracy, this new era heralds an unparalleled ability for decision makers to observe the battlespace, analyze events, and distribute information. Of critical recognition is that this era encompasses both inherent advantages and vulnerabilities, due to the interdependence of government and private sector information systems.

The military no longer operates in a completely isolated information environment. The various communication infrastructures which comprise today's information environment

---

[28] A STRATEGY, *supra* note 6, at 1.

[29] Id.

are extremely interdependent. The global information environment (GIE) is the information environment in which all organizations, individuals, or systems, "most of which are outside the control of the National Command Authorities," collect, process, and disseminate information to national and international audiences.[30] All military operations occur with the GIE, which is "both interactive and pervasive in its presence and influence," and permit aspects of such military operations to be made known to the global audience in near-real time and without the benefit of filters.[31] The Global Information Infrastructure (GII) is the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It includes a wide range of equipment,[32] physical facilities used to store, process, and display information; and the personnel who handle the transmitted information.[33] The National Information Infrastructure (NII) is similar in nature to the GII, however, it relates only to the national information environment.[34]

Of primary concern to DoD is the Defense Information Infrastructure (DII). This infrastructure is composed of shared interconnected computer systems, communications, security, data appellations, people, training, and other support structures serving DoD's local,

---

[30] FM 100-6, *supra* note 5, at 1-2.

[31] Id., at 1.

[32] The GII equipment includes cameras, scanner, keyboards, facsimile machines, computers, switches, compact disk, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, television, monitors, and printers among others. JCS PUB. 3-13, *supra* note 5, at I-24.

[33] Id.

[34] Id., at I-25.

nation, and worldwide information needs.[35] This systems carries DoD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services.

The United States' dependence on both military and civilian information and information systems is a sharp, dual edged sword. On one side are the tremendous enhanced opportunities and capabilities which stem from the incredible advancements in communications technology, while on the other side are the vulnerabilities which expose the user to a complete range of threats -- computer hackers, criminals, vandals, terrorists, and even nation states. "National security in the Information Age poses significant challenges for the Department of Defense and the nation. All organizations and decision-makers, while embracing the advantages offered by information-based technologies, must respond to the significant vulnerabilities inherent in the systems upon which their capabilities depend."[36]

DoD and all of its Service components have been and are continuing to develop technology and systems to increase the lethality of information-based systems technology in offensive information operations, while at the same time striving to diminish the capability of any potential adversaries through protective defensive information operations. The dichotomy of use of information-based systems is a fundamental aspect of what is now

---

[35] Id., at I-23.

[36] Vice Admiral Arthur K. Cebrowski, Director for C4 Systems, Joint Staff; Lieutenant General Ervin J. Rokke, President, National Defense University, in Memorandum, Subject: Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 4 July 96, in INFORMATION WARFARE: LEGAL, REGULATORY, POLICY AND ORGANIZATIONAL CONSIDERATIONS FOR ASSURANCE, (2nd ed. 4 July 1996).

known as "information operations." Use of information-based technology systems during the Gulf War prompted DoD to increase dramatically research and development in this area.[37] DoD is continuing to harness the full scope of the capabilities and vulnerabilities of information-based technologies and systems. Gathering, exploiting, and protecting information have been critical elements in command, control, and intelligence throughout history. In the future, the importance of information will not change. "What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology. While the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact."[38]

Information operations apply across the spectrum of military operations and at every level of warfare. Information operations may be employed to achieve national objectives without resorting to force or to act as a force multiplier in the event force is required. For

---

[37] ALAN D. CAMPEN, THE FIRST INFORMATION WAR: THE STORY OF COMMUNICATION, COMPUTERS, AND INTELLIGENCE SYSTEMS IN THE PERSIAN GULF (Alan D. Campen, ed., 1992) (this is a frequently cited reference on the role of information, communications, command, control, and electronic warfare in the Persian Gulf War. It consists of twenty-three articles discussing the use of knowledge and information during the Gulf War. Campen states that by "leveraging information, U.S. and Allied forces brought to warfare a degree of flexibility, synchronization, speed, and precision heretofore unknown . . . [and thus] . . . knowledge came to rival weapons and tactics in importance giving credence to the notion that an enemy might be brought to its knees principally through destruction and disruption of the means for command and control.") Id., at ix – x. *See also* Steven D. Zink, *The Information Superhighway Is A "Quivering Oxymoron" and Other Musings on Government Information Policy in an Era of Rapidly Evolving Information Technologies: An Interview with Information Futurist, Paul Saffo*, 22 JOURNAL OF GOVERNMENT INFORMATION 289, 295 (1995) ("We didn't knock the anti-aircraft batteries out, we knocked out the central coordination stations for the batteries. The 117 Stealth fighter itself was designed to deprive the enemy of key information by not appearing on radar screens. The whole thing was about info-war.").

[38] JOINT VISION, *supra* note 6, at 16.

DoD, the ultimate strategic goal of offensive information operations is to affect a human decision maker to the degree that an adversary will cease actions threatening to US national security interests. At the tactical and operational levels, information operations target and protect information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems.[39]

The concept of information dominance or superiority is the key element for operating effectively within this new environment of interdependent information systems. Information dominance/superiority is the capability "to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[40] To achieve information dominance, the commander "must be able to dominate both the traditional maneuver-oriented battlefield and the *military information environment*," defined as that "portion of the GIE relevant to his operation."[41] To achieve the latter, the commander directs the acquisition, use, and management of friendly and enemy information and conducts command and control warfare (C2W) attack and protect operations.

Information operations conducted during periods of conflict or war are called information warfare operations.[42] Information warfare can be waged in wartime "within and

---

[39] JCS PUB. 3-13, *supra* note 5, at I-2.

[40] FM 100-6, *supra* note 5, 1-1.

[41] JCS PUB. 3-13, *supra* note 5, at I-20.

[42] Id., at I-20.

beyond the traditional military battlefield."[43] As a subset of information warfare, command and control warfare (C2W) is an application of information warfare in military operations that specifically attacks and defends the command and control (C2) target set.[44] It should be noted that the capabilities and disciplines employed in C2W such as psychological operations (PSYOP), deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, can be employed to achieve effects outside of the C2 target set.[45]

The threat in the information age is unique. The systems and capabilities of the information age are evolving at blinding speed, with computer power doubling every eighteen months or less, and evermore-powerful hardware becoming available to potential "bad actors" for a low entry cost. It is estimated that over one hundred countries have the technology to attack U.S. commercial and military information systems.[46] Furthermore,

---

[43] Id., at I-3.

[44] Id.

[45] Id., at I-4.

[46] *Attacks Show U.S. Information Systems Not Immune to Information Warfare*, AEROSPACE DAILY, May 8, 1995, at 207 (The Co-Chair of the Defense Science Board task force on information for the battlefield, James O. McCarthy, a retired Air Force General, said that "there are many countries capable of conducting information warfare and the U.S. systems have been attacked in the past. More than 100 nations have the technical capability to attack the U.S. information systems and some 50 or so have done so in the past or are doing so now." Moreover, in addition to governments, there are underground groups of computer experts and individual hackers also warranting attention. A key problem in this area is the difficulty in damage assessment. "How do you find out how crippled your system is."). *See also* Gary H. Anthes, *U.S. Easy Target for Cyberattacks*, COMPUTER WORLD, May 27, 1996, at 7 ("The U.S. Congress looked at security in cyberspace last week and found it wanting. For example, federal investigators told a Senate hearing that U.S. Department of Defense computers were attacked some 250,000 times last year, with most of the assaults going undetected. But the Senate hearing on "information warfare," raised more questions than it answered. "Our government's traditional national security threats have been defined geographically," said Sen. Sam Nunn (D-Ga), a military specialist. "But when we move

there is evidence that at least half of these have attempted to penetrate these systems.[47] Their intrusions range from simply looking around the system, to destroying systems and perpetrating fraud on the telephone and banking institutions.[48] Statistics indicate that an estimated that three hundred people a day attempt to intrude into the Pentagon's computer systems.[49] Due to the speed at which these intrusions occur, it is extremely difficult to know when a system is under attack. Therefore, there may never be an opportunity to identify the intruder.

Although this thesis focuses on the relations between states, it is important to understand that in the Information Age the enemy can be any person, group, or nation. The enemy can come from anywhere. They enemy may be from within a country or organization. Among the potential targets of terrorist groups or enemy states might be the nation's power grid, the public telephone switching system, the stock markets, the Federal Reserve, the Internal Revenue Service, "strategic" companies, the research-and-development

---

from the physical world into cyberspace . . . is the bad actor a 16 year-old, a foreign agent, an anarchist, or a combination thereof?" Regarding the Pentagon security breaches, the General Accounting Office declared, "[a]t a minimum, these attacks are multimillion-dollar nuisance; at worst, they are a serious threat to national security." Nearly two-thirds "of the attacks last year were successful, meaning the hacker penetrated the system but less than 1% were detected and reported, the GAO said. The majority of the attacks were against systems carrying sensitive but unclassified information. Experts said commercial systems are at risk from terrorist attack as well. Particularly juicy targets include the information systems that support electronic fund transfers, air traffic control, power distribution and telecommunications.").

[47] Pat Cooper, *In Cyberspace, U.S. Confronts An Illusive Foe*, DEF. NEWS, Feb. 13, 1995, at 1 (hereinafter Cooper).

[48] Id.

[49] Stacey Evers, *IW Poses Infinite Questions, Few Answers*, AEROSPACE DAILY, Jun. 23, 1995, at 472 [hereinafter *IW Poses*].

structure, the air traffic control system, and the national banking system. Some have asked the question "What if Saddam Hussein, prior to his invasion of Kuwait, had hired 20 hackers to disrupt the American economy?" He would have drastically changed how the United States would have responded if he possessed the right capability to shut down the phone system by crippling AT&T's network, and destroying the financial network.[50]

Like government, private industry is vulnerable to the threats of the information age."[51] The former director of the National Security Agency, Vice Adm. John M. McConnell, USN, (Ret.), conducted experiments to see the vulnerability of the nation's supposedly "secure" computer systems. He concluded that some could be cracked "with $10,000 worth of equipment, a half-dozen college students, some pizzas, and beer."[52] "While the scope of the problem largely is speculative, hacker attacks cost U.S. business between $100 billion and $300 billion each year," said Dr. Fred Giessler, Professor of Information Warfare at National Defense University, Fort Mc Nair, Washington, D.C. This is of definite concern to the government because "[f]raud on this scale constitutes a threat to national security."[53]

---

[50] "What if Saddam Hussein had hired 20 hackers in August 1990, just before Desert Storm, to disrupt the American economy," Rep. Newt Gingrich, R.-Ga., said Speaker of the U.S. House of Representatives. "He could have shut down the phone system by crippling AT&T's network," and destroyed the financial network, which would have changed drastically how the Gulf War was waged. Cooper, *supra* note 48.

[51] *IW Poses*, *supra* note 50, at 473.

[52] John A. Tirpak, *The New Roles of Information Warfare*, AIR FORCE MAG., Jun. 1996, at 30.

[53] Cooper, *supra* note 48, at 2.

Despite the fact the that current Internet system is a result of the internet system DoD developed in the late 1960s to link research laboratories, universities, and the Pentagon, there are indications that DoD is concerned with the growing popularity of computer networks, such as the Internet, and how these systems make defense data and systems more vulnerable. The Internet computer network links more than 160 countries and has hundreds of millions of users. It carries financial and military information systems, for example, as well as personal communications.[54] The problem for the Defense Department is that in order to share information, Pentagon systems must be linked to the commercial information infrastructure through the commercial telephone communications system and the Internet. Because of the Internet's size, this means an attack could come from anywhere. It also means an attack launched by a US agent can go anywhere.

The threat situation is difficult to address because the nature of the threat has not been determined fully. For DoD this is a critical point in dealing with command and control warfare (C2W). The information-based systems which provide DoD with incredible capabilities to strike at the C2W elements of an adversary are the same ones which may be used against DoD.

While there are obvious advantages to having these advanced information-based technologies in an increasingly competitive global environment, the availability and relatively low cost of these technologies greatly increases the likelihood that potential

---

[54] Id.

adversaries will employ them also.[55] Advancements in technology have equalized the battlefield or battlespace, for smaller, less wealthy nations who do not have the capability to present a global challenge with conventional weapons. Consequently, the United States, as well as other nations,[56] are developing means to operate in this equalized battlespace such as

---

[55] *See* Senator Sam Nunn (D-Ga.), Statement at Hearing of the Senate Governmental Affairs Comm. June 25, 1996, quoted in *Cyberstrategic Attacks*, AIR FORCE MAG., Sept. 1996, at 48 ("Our intelligence agencies have acknowledged that potential adversaries throughout the world are developing a body of knowledge about the Defense Department and other government computer networks. According to these DoD officials, these potential adversaries are developing attack methods that include sophisticated computer viruses and automated attack routines [that] allow them to launch untraceable attacks from anywhere in the world. Our government understands that many countries are developing offensive information-warfare capabilities . . . At some point, we must consider how we would respond to an actual attack if one were to happen . . . . I'm not speaking of military force, but I'm speaking of perhaps using some of the tools of information warfare to basically back up on a system that carries out the attack, so that the information system itself is the subject of very severe punishment and counterattack, wherever it's coming from . . . If we don't think in that vein, then we're just basically going to be in the game-playing where everybody tries to hit us and it becomes a game as to how we can defend against it. It seems to me we've got to leap into the thought process . . . of trying to use information warfare itself to be able to make an attack or even a serious illegal probe very unattractive to the potential perpetrator.").

[56] Mary C. Fitzgerald, *Russian Views on Information Warfare*, ARMY, May 1994, at 57 (discussing the new Russian military doctrine which reflects the ongoing civil-military consensus on the nature and requirements of the new military-technical revolution (MTR) in military affairs. Russian military superiority in the MTR proceeds from superiority in information weapons, which are reconnaissance, surveillance and target acquisition (RSTA) systems, and "intelligence" command and control systems. The Russians look to the Gulf War as a basis for their concepts. The transitional nature of the Persian Gulf War was manifested in the fact that it marked the origin of certain new forms and methods of operational and tactical actions such as the electronic-fire engagement, remote-control battle, air-assault raids, an deep mobile operations.). ROBERT GARIAN, FEDERAL RESEARCH DIVISION LIBRARY OF CONGRESS, INFORMATION WARFARE: RUSSIA, FRANCE, AND THE UNITED KINGDOM (November 1995) ("Russia, France, and the United Kingdom are experiencing [information warfare]. Russia's military doctrine appears to take the Gulf War as the primary example of the future of warfare. France is heavily engaged in economic warfare, and the U.K. is taking steps to secure its information systems against a wave of serious terrorist activity on its networks. From all indications international low-level [information warfare] is a reality, and cyberwar is on the drawing boards."). *See also* Richard Behar, *Who's Reading Your E-Mail? As the World Gets Networked, Spies, Rogue Employees, and Bored Teens Are Invading Companies' Computers to Make Mischief, Steal*

information operations. These operations involve actions that can cross all phases of a military mission, the complete range of military operations, and occur at the tactical, operational, and strategic levels of warfare.[57] There are no definitive lines between these

---

Trade Secrets -- Even Sabotage Careers, FORTUNE, February 3, 1997, at 56 (In February, 1996, FBI Director Louis Freeh told a Senate panel "that 23 countries are engaged in economic spying against American business, succeeding some cases with a few keystrokes." Major culprits include: China, Canada, France, India, and Japan. "At least seven countries are training intelligence agents to hack U.S. computers for commercial data."). *See Indian Defence Experts Push For More Military Spending in Budget*, AGENCE FRANCE PRESSE, February 26, 1997, *available in* LEXIS, News Library, Afp File ("The Deputy Director of the Institute of Defence Studies and Analysis, Uday Bhaskar said that 'we will have to acknowledge that there has been a revolution in military affairs with information warfare and space surveillance being top of the agenda, and this budget has to focus on them.'"); Jason Hobby, *Cyber Leeches*, COMPUTER WKLY., December 5, 1996, at 46 ("India and Malaysia are increasingly where software is developed with little or no guarantee as to the security of the product."); Vivek Raghuvanshi, *Indian Army Hikes Info Tech Funding*, DEF. NEWS, November 3, 1996, at 8 ("Indian forces are embracing information technology from troop training to more sophisticated electronic warfare tactics."); Barbara Opall, *Study Pits PLA Nukes Against U.S., Taiwan*, DEF. NEWS, September 23, 1996, at 10. ("A purely speculative warfighting scenario circulating among Pentagon officials, intelligence analysts, and China experts shows a technologically inferior People's Liberation Army (PLA) using nuclear weapons to fry electronic circuitry on Taiwan and attack the U.S. Seventh Fleet patrolling the Taiwan Straits. But because of China's lack of adequate command, control, communications, and intelligence capabilities, limited logistics and infrastructure and inferior training, a surprise assault is 'flatly impossible' anytime in the next decade . . . . Therefore, attention must be focused on China's potential use of nuclear weapons and information warfare – an electronic blackout strike – as a means of achieving warfighting parity with the United States and Taiwan. Jencks noted that electromagnetic pulse (EMP) form a large nuclear explosion is the only known way to massively blackout electronics across a large area.");

[57] A brief explanation of the strategic, operational, and tactical levels of warfare is essential to understanding how, when, and by whom information operations may be used. Military attorneys at all levels of military operations need to be aware of information operations and the legal and policy concerns connected with them. While military attorneys operating at the strategic levels will primarily be involved in information operations, attorneys at both the operational and tactical levels may also become involved in such operations. Activities at the strategic level of warfare establish national and multinational military objectives; sequence initiatives; define limits and assess risks for the use of military and other instruments of national power; develop global plans or theater war plans to achieve these objectives; and provide military forces and other capabilities in accordance with strategic plans. JOINT CHIEFS OF STAFF, PUBLICATION 1-02, DICTIONARY OF TERMS 397 (1993) [hereinafter JCS PUB. 1-02]. At the strategic level of warfare, which is the focus of this thesis, both military

and national leaders can use information operations as an integrating national strategy which focuses upon using information operations in peacetime to avoid going to kinetics or conflict. Developing such an information operations capability will enable strategic planners to focus on using information operations in peace and crisis to prevent war. JCS Pub. 3-13, *supra* note *5*,, at II-18. For example, an information operation could assist in setting the conditions for a peaceful transition to a more democratically inclined form of government. At the strategic level, this will require a process that will allow interagency operations, particularly in peace, to make a comprehensive use of information operations. Normally, the National Command Authority (NCA), the President and Secretary of Defense or their designated representatives (JCS PUB. 1-02, at 236) will direct information operations at the strategic level. Such operations will be planned in coordination with other agencies or organization outside of DoD. At this level, information operations "seek to engage adversary or potential adversary leadership to deter crisis and end hostilities once they occur." JCS PUB 3-13, *supra* note 5, at II-18. These operations would be employed to influence or affect all elements – political, military, economic, information – of an adversary's national power. JCS Pub. 3-13, *supra* note *5*,, at II-19. When tasked by the NCA, a combatant commander (a commander-in-chief of the unified or specified command established by the President) (JCS PUB. 1-02, at 56), within an assigned area of responsibility (AOR) may conduct offensive information operations in support of strategic security objectives. JCS Pub. 3-13, *supra* note *5*, at II-19.

The Joint Chiefs of Staff maintain that "information operations can support the overall United States Government (USG) strategic engagement policy throughout the range of military operations. The effectiveness of deterrence, power projection, and other strategic concepts is greatly affected by the ability of the US to influence the perceptions and decision-making of others." (A STRATEGY, *supra* note 6, at 5). In periods of crisis, information operations can aid in deterring "adversaries from initiating actions detrimental to the interest of the US or its allies or to the conduct of friendly military operations. If carefully conceived, coordinated, and executed, information operations can make an important contribution to defusing crisis; reducing the period of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts, and forestalling or eliminating the need to employ forces in a combat situation. Thus, both information operations in peacetime and information warfare in crisis and conflict, at both the national-strategic and theater-strategic levels, require close coordination along with various government agencies including DoD.

Activities at the operational level of warfare link tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time and space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives. JCS PUB. 1-02, at 302. Activities at the tactical level of war focus on the ordered arrangement and maneuver of combat elements in relation to each other and tot he enemy to achieve combat objectives. This is the level where battles and engagements are planned and executed to accomplish military objectives. JCS PUB. 1-02, at 411.

operations, which makes it challenging to categorize them for purposes of applying international law of peace and armed conflict, particularly those operations that fall in "peacetime."

A. *Definitions of Information Operations*

During the past several years, in the absence of a national level definition of information operations, many writers attempted to define the nature of information operations and posited several definitions.[58] According to the most current DoD definition released in 1996, information operations are "actions taken to affect adversary information, and information systems, while defending one's own information and information systems."[59] What is particularly interesting about this definition is that it does not mention spatial dimensions such as space, air, land, or sea; it merely describes the nature of the activity, without restricting it to any particular realm. This is a critical issue in the area of international law. The new informational domain of cyberspace overlaps and intersects these

---

[58] Dr. Martin Libicki, Professor of Information Warfare at the School of Information Warfare Studies at National Defense University, proposed seven alternative definitions and taxonomies for twenty-first century warfare while the higher level policy documents of DoD and the Joint Staff were under revision: (1) command-and-control warfare (C2W); (2) intelligence-based warfare (IBW); (3) electronic warfare (EW); (4) psychological operations (PSYOPS); hacker warfare – software-based attacked on information systems; (6) economic information warfare (EIW) – war via the control of information trade; and, (7) cyberwarfare - combat in the virtual realm. LIBICKI, *supra* note 6, at 7. *See also* Arquilla, *supra* note 6, at 24 (John Arquilla and David Ronfeldt introduced the terms "cyberwar" and netwar" in their paper *Cyberwar is Coming!* They argue that mass and mobility will no longer decide the outcome of conflict. Instead, decentralized, networked forces with superior command, control, and information systems will disperse the fog of war while enshrouding the enemy in it. They provide an example excellent of successful employment of "cyberwar" by the twelfth and thirteenth century Mongol armies.).

more traditional and familiar spatial dimensions of the battlefield. Historically, the dimensions of space, air, land, and sea allow for different actors and their weapons. The dimensions of cyberspace, however, are not conducive to such discrimination.

It is common to see the term information warfare still used in discussion in this area. Information warfare was the term used before DoD's adoption of the term information operations. As the term "warfare" could engender negative connotations and perceptions about the use of information and information systems, DoD changed the term from information warfare to information operations in order to have non-threatening nomenclature which could be used in discussions with both government and non-government organization and agencies.[60] DoD now uses the term information warfare to define only those offensive "information operations conducted during a time of crisis and conflict to achieve a military objective over a specific adversary or adversaries."[61] Doctrinally, "[i]nformation operations will require the close integration of offensive and defensive capabilities and activities, as well as effective design, integration, and integration of command and control with intelligence support. Information Operations are conducted through the integration of many disciplines."[62]

---

[59] JCS Pub. 3-13, *supra* note *5*,, at I-17.

[60] I learned this history of the terminology switch from my interviews with Colonel John Burton. Interviews with Colonel John Burton, Legal Counsel, Chairman's Legal Counsel Office, in Pentagon, Washington, D.C. (Oct. 1996; Jan. 11, 1997). See JCS Pub. 3-13, *supra* note *5*,, at I-20.

[61] Id.

[62] JCS PUB. 3-13, *supra* note 5, at I-17-18.

B. *The Use of Information Operations*

Information operations can be conducted in both the offense and defense, but the element of information operations that causes the most consternation to policy makers and legal scholars is the offensive use of information operations.[63] Some offensive methods of information operations may seem to be the products of science fiction. Attacks can be conducted from a distance, through radio waves or international communications networks, with no physical intrusion beyond enemy borders. This particular aspect of information operations lies at the heart of the international law conundrum that will be discussed in Section III. The effects of such cyberspace intrusions could range from the denial of services of important military or governmental systems in time of crisis, or military or civilian deaths from system malfunctions, to widespread fear, economic hardship, or merely inconveniences for civilian populations who depend upon information systems in their daily lives. It can be as simple as primitive propaganda and deception actions to high tech viruses and morphing techniques. It is a concept that can be employed offensively, defensively, across the entire spectrum of military operations.

---

[63] All information gathered for this thesis about offensive information operations is from unclassified sources. *See supra* note 3, and accompanying text. *See e.g., Air Force Hacker Hits Navy,* INTEL. NEWSL., Oct. 12, 1995, no. 273 (Air Force General John Fitzgerald, Deputy Chief of Staff for Command, Control, Communications and Computers, stated in an interview with DEFENSE NEWS that the U.S. was also capable of taking the offensive to cause serious damage by electronic penetration. "I can't tell you what we are doing on the offensive side of information warfare but it's much more than the study phase," he said. And he added: "If you wanted to shut down the electrical grid system in Baghdad and the weather was such you couldn't put up airplanes that day you turn to information warfare.").

Information operations are deliberate actions to control and manipulate an adversary's information and information systems. These operations affect the other party's "truths" or "known elements" for decision making purposes.[64] Manipulation of the "truth" can have varied effects as it is applied across the phases of an operation or range of operations, and at every level of warfare. Offensive information operations are conducted during crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Defensive information operation activities are conducted on a continuous basis, in both peacetime and war, and are an inherent part of force employment across the range of military operations.

There are two components of information operations: offensive and defensive. The combination of offensive and defensive information operations achieves information superiority.[65] Defensive information operations provide the "capability to collect, process and disseminate an uninterrupted flow of information" while offensive information operations exploit or deny an adversary's ability to do the same.[66]

1. *Defensive and Offensive Information Operations* -- Information operations are divided into two areas, offensive (attack) and defensive (protect). Defensive information

---

[64] "Truth is not reality but a perception of reality." Statement made by the character Cosmos in the motion picture SNEAKERS (UNIVERSAL 1992). *See supra* note 2 and accompanying text.

[65] JOINT VISION, *supra* note 6, at 16.

[66] *See* JCS PUB. 3-13, *supra note* 5, at I-19.

operations, the term used in this thesis, is also known as information assurance.[67] This distinction between offensive and defensive operations is very important when determining the net effect of information operations, which can occur simultaneously. A further distinction between defensive and offensive information operations is that defensive operations are regulated mostly by domestic law while offensive operations are regulated mostly by international law. Although defensive and offensive information operations may produce the same result, the intended purpose of each operation will be a distinguishing factor in determining the legality of the operation.

The common link between the two types of operations is the target sets involved. Both operations can be employed at all levels of military operations and across the entire spectrum of military missions. Both operations must be carefully integrated to provide timely response against identified and potential threats to friendly information and information systems.[68]

a. *Defensive Information Operations* -- Defensive information operations ensure the necessary protection and defense of information and information systems. "In

---

[67] *See* Science Application International Corporation, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance 1-1 (2nd ed., July 4, 1996). *See also From "Information Security" to "Information Assurance"*, C4I News, Aug. 1, 1996, *available in* WESTLAW 1996 WL 8434836; James Kerr, *Information Assurance: Implications to National Security and Emergency Preparedness, in* Cyberwar: Security, Strategy, and Conflict in the Information Age, 257 (Alan D. Campen, et al. eds, 1996); Science Application International Corporation, *Planning Considerations for Defensive Information Warfare - Information Assurance* (December 16, 1993).

[68] *See* JCS PUB. 3-13, *supra* note 5, at III-3.

war, the defensive exists mainly that the offensive may act more freely."[69] Doctrinally, these operations integrate and coordinate policies and procedures, operations, personnel, and information assurance technology to protect information and information-based processes and systems.[70] They prevent intrusions or attacks upon the decision makers, the information, and information-based processes upon which they rely, and the decision makers means for communicating their decisions. Defensive information operations aim to prevent an intruder from "pushing" their information operation through the system[71]

Understanding the nature of a defensive measure which may be employed in response to an intrusion is critical to knowing whether such a response is legally permissible. Our initial response capabilities have advanced over the past several years, however, not at the same rate of speed at which the technology to intrude an information system has progressed.[72] The desire to improve our defensive posture has prompted the development of automated intrusion detection capabilities or active defensive measures. These capabilities will automatically detect system intrusions and instantly generate alerts. Some proposals even include launching automatic crippling responses back through the network system into the intruders computer.[73]

---

[69] Mahan, Rear Admiral Alfred Thayer, NAVAL STRATEGY (1911), *in* HEINL, ROBERT DEBS, JR., DICTIONARY OF MILITARY AND NAVAL QUOTATIONS 83 (1966).

[70] *See* JCS PUB., *supra* note 5, at III-2.

[71] DAVID S. ALBERTS, NAT'L DEF. U., DEFENSIVE INFORMATION OPERATIONS 4 (1996).

[72] JCS PUB. 3-13, *supra* note 5, at III-16.

[73] *Age of Anarchy in Cyberspace,* SOUTH CHINA MORNING POST, February 19, 1997, at 13 ("The Defense Science Board Task Force report calls for 'hot pursuit' as an option, how can you distinguish a hired attacker from a bored suburban kid? Treating all intruders as the

Defensive information operations can be divided further into passive defensive measures and active defensive measures.

(1) *Passive Defensive Measures* -- Passive defensive operations usually do not raise many legal issues. They are non-intrusive measures of protection. This would include basic techniques of concealing prime targets, hardening targets against intrusion, developing and providing backup systems. This could be as simple as ensuring compliance with information security procedures and practices and encrypting data. It could also mean developing the technological capability to maneuver out of the way of an intruder.[74] These activities should be employed throughout tactical, operational, and strategic levels of the information infrastructure.

(2) *Active Defensive Measures or countermeasures* -- While a passive defensive operation utilizes measures to protect the intruder from gaining access, an active defense operation is one that actually attacks the intruder in some manner. While the legal principles which govern the use of physical force to defend persons and property are well established, some assert that domestic and international law do not adequately address the

---

enemy is a good way of turning the curious into the hardcore malicious. Like other technological problems, security demands not massive force, but new techniques for making systems more robust and even self-healing. Procedures for civil defense risk an illusion of control that can ultimately be self-defeating."). *See generally* Stacey Evers, *Stopping The Hacking Of Cyber Information,* JANE'S DEF. WKLY., Apr. 10, 1996, at 22.

[74] PRIMER, *supra* note 6, at 5.

legality of active defense measures permitted to defend elements of the cyberworld.[75] Such an assertion is only partially accurate.

While domestic laws on this topic may not exist, or the laws that do exist only partially cover certain situations, there are appropriate domestic mechanisms which allow for correction of these deficiencies.[76] In the international law arena, however, such mechanisms are not readily available. Therefore, reliance upon the world community's past experience in dealing with similar situations is essential. Justice Oliver Wendell Holmes, the great American jurist, opined that "the life of the law has not been logic: it has been experience."[77] The incrementalist approach to international law looks to past experiences and resultant legal determinations in dealing with similar experiences. The conventional methods of active defense against intrusion such as use of mine fields and trip wire warning devices provide a basis upon which to analyze active electronic mechanisms to deter intrusion.

---

[75] Id.

[76] The Department of Justice is working to alter existing legislation that hinders operations to identify, surveil, and apprehend intruders. Interview with Mr. M. E. "Spike" Bowman, Associate General Counsel, National Security Affairs, Federal Bureau of Investigation, Washington, D.C. (Jan. 30, 1997). *See also* Bowman, *supra* note 6.

[77] OLIVER W. HOLMES, THE COMMON LAW 1 (1881). BERNARD SCHWARTZ, A HISTORY OF THE SUPREME COURT (1993). Justice Holmes' lectures on the topic of the common law were published in a book by that name in 1881. This book was to change both Holme's life and the course of American law. Holmes rejected the notion that "a given [legal] system . . . for instance, can be worked out like a mathematics." Instead, Holmes declared, "The law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained the axioms and corollaries of a book of mathematics." Holmes theme was stated at the very outset of *The Common Law*: "the life of the law has not been logic: it has been experience. The felt necessities of the time, the prevalent moral and political theories, intuitions of public policy, avowed or unconscious, even the prejudices which judges share with their fellow-men, have had a good deal more to do than the syllogism in determining the rules by which men should be governed." Id., at 191 (footnotes omitted).

In the cyber realm, an electronic intruder may activate a mechanism which detects the intruder and attacks his or her equipment electronically. This is also known as hack-back defense measures.[78] The activation of this system could be automatic or controlled by an operator. There is clearly a preference for having a human in the loop on systems which active defense systems which protect property.[79]

Use of warnings is extremely important if there are active defensive measures in place. Such warnings may actually deter the intruder from entering and provide a defense to a liability claim. They would serve notice to the intruder that there is a risk of encountering an active defense system measure which may cause damage to their systems if they proceed further. In essence, a warning message could be a sort of "beware of the junk yard dog, enter at your own risk"[80] message to warn off the intruder.

Unfortunately, such warnings only work against those intruders who enter the system through the front door. Those intruders who are capable of bypassing normal entry procedures and enter through the "back door," would not have the "benefit" of the warning.

---

[78] Hack-back and hot pursuit are terms used to describe a technique in which the system, which is invaded, can strike back at the intruder (hacker). *See generally* David W. Methvin, *Safety on: Protect Yourself From Hackers, Crackers, and Outlaws,* WINDOWS MAG. 164 (Aug. 1996); John J. Fialka, *Pentagon Studies Art of "Information Warfare" to Reduce Its Systems' Vulnerability to Hackers,* WALL ST. J., Jul. 3, 1995, at 20.

[79] PRIMER, *supra* note 6, at 6.

[80] Comment made by Dr. Fredrick Giessler a Professor at the School of Information Warfare Strategy of the National Defense University, Ft. McNair, Washington, D.C., during the

It is unlikely that such an intruder would be successful in establishing a claim against the "owner" of the system for damage caused by any active defense system in light of the unauthorized entry. Despite the unauthorized entry, the level of damage or net effect of the active defense measure will weigh heavily in determining the liability level.[81]

An aspect of active defensive measures which is also applicable to offensive measures is that we do not have the technology right now to know the end result of an attack that is launched.[82] A critical problem arises based upon two points: (1) information and information systems are deeply interconnected, and (2) most intruders set out upon a most circuitous route before actually intruding into a system. Because our technology is still developing, we do not have the complete capability to determine the ultimate result of an active defensive hack-back response through a system. Only when we have the capability to determine this will such responses be accurate.

With active defensive measures, attorneys will have to determine whether a response action is legal. Ascertaining the identity of the initial intruder and the nature of that intrusion will ultimately affect the conclusion whether the active defensive response was appropriate

---

Intermediate Information Warfare Course, School of Information Warfare Strategy, National Defense University, Ft. McNair, Washington, D.C., (Mar. 6, 1997).

[81] *See* Katko v. Briney, 183 N.W.2d 657 (Iowa 1971) (awarding punitive damages to plaintiff who, while trespassing on defendant's land, triggered defendant's spring gun).

[82] Interview with Major Steve Spano, J6, Joint Staff, at the School of Information Warfare · Strategy, Nat'l Def. U., in Ft. McNair, Washington, D.C. (Mar. 4, 1997); and, Interview with Lieutenant Colonel Joseph Rakosky, J-38, Joint Staff, at the School of Information Warfare Strategy, Nat'l Def. U., in Ft. McNair, Washington, D.C. (Jan. 31, 1997).

and legal.[83] Thus, improper active defense measures could result in individual criminal and civil liability to the launcher or even set two nations on the brink of crisis. The major legal concern with active defense measures distills to the fundamental premise that the end effect of the response will determine its legality.

b. *Offensive Information Operations* -- Offensive information operations focus upon the vulnerabilities and opportunities presented by an increasing dependence on information and information systems. States may use information operations to affect an adversary's or potential adversary's use of or access to information and information systems.[84] Offensive information operations rely upon traditional perception management disciplines to include

---

[83] It is extremely important to understand that there is no clear dividing line between information operations that fall within the purview of criminal law and those that fall within the realm of international law. These intrusions occur extremely quickly and, in many instances, anonymously. The inability to identify quickly and accurately the identity of an intruder and also ascertain the nature of their intrusion, poses a great challenge to government agencies. Only when these questions are answered, can the appropriate agency or department respond. Nevertheless, until that can occur, precious time is lost. Interview with Mr. M. E. "Spike" Bowman, Associate General Counsel, National Security Affairs, at Federal Bureau of Investigation, Washington, D.C. (Jan. 30, 1997); Interview with Special Agent Jim Christy, Senate Investigator (Congressional Fellow), at National Defense University, Ft. McNair, Washington D.C. (Mar. 4, 1997); Telephone interview with Martha Stansell-Gamm, Deputy Chief of Computer Crime and Intellectual Property Division, Department of Justice, on (Mar. 10, 1997). *See also* Scott Charney and Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931 (1996) ("More importantly, the launching of malicious programming codes through global computer networks and international hacker attacks is no longer the fanciful idea of science fiction writers and screenwriters; it is existing policy. Often termed 'computer crime,' the offenses actually are the product of a merger between two related but distinct technologies – computers and telecommunications. The criminal potential is enormous, and the Justice Department's introduction to crimes committed in cyberspace was indeed a startling one."). Vic Sussman, *Policing Cyberspace: Cops Want More Power to Fight Cybercriminals,"* U.S. NEWS & WORLD REP., Jan. 23, 1995, at 54-60 ("The day is coming very fast when every cop will be issued a badge, a gun, and a laptop.").

psychological operations (PSYOPS), deception, jamming, signals intelligence (SIGINT), and physical or electronic attack on enemy information systems.

This includes both traditional methods, such as a precision attack to destroy an adversary's command and control capability, and nontraditional methods such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers.[85] These operations involve the "pushing" of our information towards the adversary.

The goal of information operations is to maintain peace, defuse crisis, and deter conflict.[86] Offensive information operations are heralded as having the "greatest impact in peace and the initial stages of crisis."[87] Information operations impact in "perception management,"[88] – influencing an adversary's decision making – and it's highest value is in peace and military operations other than war (MOOTW).[89] Offensive information operations

---

[84] JCS PUB. 3-13, *supra note* 5, at I-18. In some instances, information operations that, by their sensitive nature and potential effect or affect, security requirements, or risk to the national security of the US, require special review and approval process. Id., at 20.

[85] JOINT VISION, *supra* note 6, at 16.

[86] JCS PUB 3-13, *supra* note 5, at II-14.

[87] A STRATEGY, *supra note* 6, at 5.

[88] MOLANDER, *supra* note 6, at 22 (Perception management is a termed used by Roger Molander in the National Defense Research Institute (RAND) "Day After . . ." exercise. "As cyberspace evolves, entry costs decrease, and the boundaries of national sovereignty are blurred, there will be increased opportunity for adept nonstate and state actors to manipulate information that is key to perceptions.").

[89] JCS PUB 3-13, *supra* note 5, at II-14.

used during time of crisis or conflict to achieve or promote specific objectives over a specific opponent are called information warfare.[90]

Contemporary literature and films provide some extremely frightening examples of potential offensive information operations capabilities.[91] Since the equipment necessary to carry out these operations is relatively inexpensive, once one possesses the knowledge to do these operations, they can be employed both offensively and defensively. Some potential offensive information operations include:

- Remotely altering via computer the formulas of medication at pharmaceutical manufacturers, or personal medical information, such as blood type, in medical databases.[92]

---

[90] Id., at I-20.

[91] While there are many non-fiction sources such as the RAND "Day After . . ." exercise results, which reveal potential offensive information operations capabilities, techniques of information warfare are also found in the plots of several movies and novels. In Tom Clancy's best-selling novel DEBT OF HONOR (1994), his main character, Jack Ryan, is back as the White House National Security Advisor. The Japanese, among other things, use a software "Easter egg" planted to cripple the stock exchange and sabotage America financially. Many recent movies have used information warfare techniques as their central theme. The main plot of the 1996 film, MISSION IMPOSSIBLE, is cyber-age crime. A retired Russian spy plans the theft of a computer disk containing the identities of the world's most estimable undercover agents. The Mission Impossible team tracks down a cyber-criminal, code-named Job, who initially sought to steal and sell computer the disc containing the information. MISSION IMPOSSIBLE (Paramount 1996). Teenagers take center stage in two other "cyber" theme movies. In HACKERS, teenage computer "techheads" put their computer skills to good use trying to stop a mysterious computer genius from destroying America's economy via CompuServe. They hack into a corporate computer system and stumble on an embezzlement scheme. HACKERS (MGM 1995). In the 1983 film, WAR GAMES, another teenager hooks his home computer into the US defense system in the Pentagon and risks the outbreak of World War III. As the government, moves to stop him their efforts are intensified after he accidentally triggers nuclear missiles firing at Russia. WAR GAMES (United Artists 1983).

[92] The motion picture THE NET (Columbia 1995) provides an example of this type of intrusion into personal records, when unknown computer intruders alter the computerized

- Using "computer hacking" techniques to insert a logic bomb into a rail computer system, causing trains to be misrouted and perhaps crash.[93]

- Inserting a computer "worm" or "virus" into a computer that could then travel from computer to computer through a network, damaging data and disrupting systems.[94]

---

medical records of a Presidential cabinet member at a military medical center. THE NET'S main character, Angela Bennett, accidentally acquires a disk that some villains want back so badly that they go after her – technologically. They erase the deed to her house and turn her "informationally" into the felon Ruth Marx. The hidden fear that drives THE NET is the creepy thought that "if Ruth, a computer guru, can't prevent what's happened to her, what hope is there for the rest of us?" THE NET (Columbia 1995).

[93] MOLANDER, *supra* note 6 (Between January and June 1995, six cyber-war exercises took place. These exercises were based on a method "The Day After . . .." pioneered by Roger Molander, a senior analyst in Rand's Office in Washington, DC. The original RAND studies were conducted during the Cold War to stimulate thinking about nuclear defense among top U.S. leaders. Dr. Molander's most recent exercises have raised more questions than answers, but the games persuaded the military's leadership to take the threat of information warfare seriously. The exercises demonstrated just how much of America's defenses – from launching missiles to mobilizing troops in an emergency – depends on civilian networks. The exercises provide examples of potential offensive information warfare techniques. They are set in the year 2000, and start out when Internet junkies in suburban Maryland notice that something has gone horribly wrong. Local computer users find it is impossible to log on to the communications network. Those already connected watch helplessly as their computer hard-drives become clogged with streams of e-mail messages containing 10,000 lines of garbage at a time. Meanwhile, managers running large information sites on the World Wide Web, a popular multimedia section of the Internet, see their big server computers grind to a halt after being overwhelmed by tens of thousands of simultaneous requests for data. Only hours later do engineers at the telephone companies, defense laboratories, and universities begin to suspect that traffic swamping the Internet connections on the East Coast of America are no accident. The tell-tale sign is the way the packets of data flooding the network keep changing their originating addresses. All that can be determined is that the malevolent data is coming from somewhere in Eastern Europe. Days later – when the lights have gone out, the telephone lines are jammed solid, trading on the New York Stock Exchange has stopped (despite the absence of snow), automated teller machines have started crediting and debiting thousands of dollars to customers' accounts at random, and airliners have lost their air-traffic control – the ghastly realization dawns. America is under attack: the victim of a cyber war.). *Cyber Wars: Logic Bombs May Soon Replace More Conventional Munitions,* THE ECONOMIST, January 13, 1996, *available in* 1996 WL 8670720 (Geoffrey Baehr, a technology guru in Silicon Valley, says a network war could halt a country's economy as effectively as an electromagnetic pulse following a nuclear detonation – and for the same reasons.).

[94] Steve Lohr, *Ready, Aim, Zap: National Security Experts Plan for Wars Whose Targets and Weapons Are All Digital*, N.Y. TIMES, Sept. 30, 1996, at D1, D2. *See also* Harris

- Deliberately initiating a concerted e-mail attack that could overwhelm or paralyze a significant network.[95]

- Hiding a "trap door" in the code controlling switching centers of the Public Switched Network, causing portions of it to fail on command.[96]

- Generating a mass dialing attack by personal computers that may overwhelm a local telephone system.[97]

- Intentionally subjecting a country to an "infoblockade," in which little or no electronic information will be able to enter or leave its information infrastructure system.[98]

- Diverting funds from bank computers, or corrupt data in bank databases, causing disruption or panic as banks shut down to address their problems.[99]

Collingwood, *A Law Strong Enough to Catch A Hacker*, BUS. WK., Feb. 5, 1990, at 34 (A federal jury in Syracuse, N.Y. found computer hacker Robert Morris guilty of violating the Computer Fraud & Abuse Act of 1986, in January 1990. Morris, a suspended Cornell University computer science student, was convicted of unleashing a software "worm" in November 1991 that wreaked havoc with computers linked to the Internet.).

[95] Diedtra Henderson, *How Hacker Stalled Traffic on Net – Deluge of Bogus Messages From Unknown Source Caused Near-Gridlock on Information Superhighway*, THE SEATTLE TIMES, Oct. 11, 1996, at A1.

[96] MOLANDER, *supra* note 6, at 64.

[97] Id.

[98] Kanuck, *supra* note 6, at 280.

[99] Molander, *supra* note 6, at 74. *See also* Gary H. Anthes, *Few Gains Made Against Hackers*, COMPUTERWORLD, September 16, 1996, at 20 (In the private sector, Stephen R. Katz, Chief Information Security Officer at Citibank NA in New York, blamed clueless users and careless vendors for successful computer attacks. "Products either lack security or are delivered with security functions turned off. Some are even delivered with hidden back doors to allow vendor maintenance personnel easy access." Russian hackers broke into Citibank systems last year and made off with some $10 million. The bank declined to say just how the cyberheist was accomplished. Katz believes that hackers have entered a dangerous third phase. In the first phase, hackers were driven mostly by curiosity.); Hugo Cornwall, *The Tale of the Russian Hacker*, THE GUARDIAN, December 5, 1996, at 5 (Everyone wants to know how Vladimir Levin did it, writes Hugo Cornwall. In mid-1994, as a 26-year-old computer scientist in St. Petersburg, Levin is supposed to have led a gang that hacked into Citibank in New Jersey, and organized more than 40 wire transfers from customer accounts. Russia's Mafia is said to have been involved. The recent case involving

- Stealing and disclosing confidential personal, medical, or financial information, as a tool of blackmail, extortion, control, or to cause widespread social disruption or embarrassment.[100]

- Taking over a radio and television network, and then using it to broadcast propaganda or other information.[101] Such intruders could use techniques such as "video morphing" to make the new broadcasts indistinguishable from the overtaken networks own usual broadcasts.[102]

Citibank is one example. Between June and October in 1994, approximately 40 wire transfers were attempted from Citibank's cash management system through the use of a computer and phone lines from St. Petersburg, Russia, by compromising the password and user identification code system. Citibank was successful in blocking most of the transfers or recovering the funds from recipient banks, limiting its losses. However, the potential loss was enormous. Moreover, imagine what the impact might have been if the intruders' intent was not to steal funds from a few accounts, but to bring down the entire bank's accounting system; or to zero out the records of thousands of accounts; or to disrupt several major banks simultaneously.); PREPARED STATEMENT BY HONORABLE JAMIE S. GORELICK, DEPUTY ATTORNEY GENERAL OF THE UNITED STATES BEFORE THE SENATE GOVERNMENTAL AFFAIRS COMM. PERMANENT SUBCOMM. ON INVESTIGATIONS, RE: SECURITY IN CYBERSPACE, Fed. News Serv., Jul. 16, 1996 ("The President yesterday signed Executive Order #13010, on Critical Infrastructure Protection. That Order creates a Presidential Commission that will formulate policy recommendations to the President – including any draft legislation – on measures to protect the nation's critical infrastructures from terrorist and other forms of attack. The Order cites two sorts of potential threats to these infrastructures: bombings and other "physical" threats to tangible property; and computer-based, "cyber" attacks on the information or communications components that control the infrastructures." The infrastructure to be protected include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. As the Executive Order states, these infrastructures are "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.").

[100] MOLANDER, *supra* note 6, at 79.

[101] Dave Moniz, *Pentagon Developing Computer Weaponry for "Information Warfare,"* PHILADELPHIA INQUIRER, Jul. 25, 1996, at 6.

[102] Grier, *supra* note 3, at 35 (Colonel Frank M. Morgan, United States Air Force (USAF), Commander, Air Force Information Warfare Center (AFIWC), emphasizes that modern video and audio morphing technology, such as that used to make the motion picture FORREST GUMP, has many potential information warfare applications. Queried for examples, the colonel suggests "letting the imagination run wild."). *See also* Braunberg, *supra* note 6, at 63.

- Of national security concern is that a nation's command and control infrastructure could be disrupted, with individual units being unable to communicate with each other or with a central command. More disrupting (and potentially more devastating), is the disruption of a nation's command and control infrastructure which separations the National Command Authority and the strategic level commanders from major subordinate commands.[103]

Other potential targets for electronic disruption or manipulation include stock or commodity exchanges, electric power grids, municipal traffic control systems, and air traffic control and navigation systems.[104]

What is important to keep in mind when considering these examples of computer based network interference is that there are many types of intruders. An intruder may be another state or government actor, which is the focus of this thesis, or it may be a non-state actor, such as an international terrorist individual or organization, or an individual or organization engaged in criminal activity for private gain, or merely bored individuals "playing" in the information infrastructure. It is critical to be able to differentiate among these actors in order to know which legal analysis is applicable – based on domestic criminal, civil, or international law. The cyber techniques of a criminal intruder, a state or government intruder, or a bored teenager may produce the same net effect; however, the law which will be applied will be different, depending on the facts.

III. The International Law of Armed Conflict and Information Operations

---

[103] This scenario illustrates an attack at the strategic level that targets the command and control center.

Public international law concerning the conflicts between nations developed through civilization's continuous struggle to regulate and alleviate the atrocities and suffering of war.[105] The body of law that evolved from the centuries of experience dealing with conflict

---

[104] John Carlin, *U.S. Fears "Electronic Pearl Harbor,"* THE INDEPENDENT, Feb. 9, 1997, at 12.

[105] A. P. V. ROGERS, LAW ON THE BATTLEFIELD 1 (1996) [hereinafter ROGERS]. Various scholars, such as Grotius, Vattel, and Victoria, are credited with contributing significantly to the development of this body of law. Hugo Grotius (or de Groot) (1583-1645) is known as the "Father of International Law." This eminent humanist from the Netherlands, who became a renowned jurist, published the famous *De Jure Belli ac Pacis* in 1625. Reacting to the barbarism and amorality of contemporary warfare and international politics, Grotius sought to establish control, discipline, and restraint both in the conduct of war and in the relationships between states within the framework of natural law. He argued that the human rights, which were discernible in natural law, remained in existence during war. For Grotius, these rules and guidelines – the decent treatment of prisoners, humanity towards civilians, respect for property, honesty in the formulation of contracts and treaties, rights for neutrals, and resort to armed conflict only for good reasons – were all based on natural law. A DICTIONARY OF MILITARY HISTORY 332 (Andre Corvisier, ed., John Childs, English rev. and expanded ed., Chris Turner, trans. 1993) [hereinafter A DICTIONARY]. Emerich de Vattel, (1714-67), published his *Law of* Nations in 1758. Vattel argued that states are equal and that the prime duty of each is national survival. The need to preserve oneself against aggressors did not, however, preclude the possibility of improvements beyond the mere struggle for survival, because it was open to states to enter into voluntary agreements with one another to limit their conflicts and to promote cooperation. Vattel was strongly opposed to the tendency for war to become punitive. He pointed out that every belligerent considers itself to be just and its opponent unjust, and that the consequence is pointless savagery; it was better, he thought to accept that war can be just on both sides. Id. at 839. Francisco de Vitoria, (c.1492-1546) was a Dominican priest and Prime Professor of Sacred Theology in the University of Salamanca and a leading figure of the Spanish theologico-juridical school, Vitoria was one of the first modern theorists of *Jus inter gentes*, a formula which, when translated by Jeremy Bentham (1748-1832), became "International Law." He wrote two books on war: *De Indis* and *De Jure Belli.* In place of the medieval notion of a universal state, he substituted that of *Res publica humana*, a universal society based on equality between states. He recognized the existence and legitimacy of *Res publica humana* on the grounds of the theological notion of humanity. He thus denied the Pope any rights over the temporal domain of princes. Vitoria expounded the theory of just war, which he adopted from St. Thomas Aquinas. Hugo Grotius was deeply influenced by the writings of Vitoria. Id., at 851-52.

and war is referred to as customary law.[106] It is referred to as such because it reflects the customs and usages of war. Eventually, society codified many of these century old customs and usages. Our contemporary international law,[107] and its subdivision governing armed conflict, is a direct result of the centuries of experience and evolution of ideas regarding conflict among nations.

As each generation has attempted to explain and advance the law regarding armed conflict in an evolutionary manner to coexist with the developments in society, they faced many challenges in dealing with the then existing framework of law and the new situations they encountered. For example, nearly fifty years ago, those who sought to revise the rules pertaining to victims of war following World War II faced new opportunities to develop and evolve international law. One scholar stated that "[i]f international law is, in some ways, at the vanishing point of law, the law of war is, perhaps even more conspicuously, at the

---

[106] *See* Horace B. Robertson, Jr., *Contemporary International Law: Relevant to Today's World?*, NAVAL WAR COLLEGE REV., Summer 1992, at 89, 93 (hereinafter Robertson) ("customary law is created by state practice. To be sure, many authorities argue that even long-continued and consistent practice does not alone create customary international law, but that something more is required: a state's belief that the practice is obligatory. Nonetheless, along-continued practice acquiesced in by other states may create customary international law irrespective of the intent of states that acquiesce."). ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, para. 5.4.1 (1989) (hereinafter ANNOTATED SUPP.) (Customary international law is "the law of armed conflict derives from the practice of military and naval forces in the field, at sea, and in the air during hostilities. When such a practices attains a degree of regularity and is accompanied by the general conviction among nations that behavior in conformity with that practice is obligatory, it can be said to have become a rule of customary law binding upon all nations."

[107] GERHARD VON GLAHN, LAW AMONG THE NATIONS: AN INTRODUCTION TO PUBLIC INTERNATIONAL LAW 2 (6th ed., 1992) [hereinafter VON GLAHN].

vanishing point of international law."[108] Another scholar extended this thought by stating "if the law of war were at the vanishing point of international law, the law of the battlefield would be at the vanishing point of the law of war."[109] It is important to note that these scholars did not indicate that the challenging situations were beyond the body of existing law, just that they were at the extremes of previous legal thoughts and experiences. Today, we are in a similar situation as we struggle to extend the framework of public international law to the newest techniques in battlespace – information operations.

A. *The Incrementalist Approach to International Law*

The current international legal paradigm is a result of an evolution through the centuries in response to experiences of the community of nations and will continue to evolve to meet future changes. The evolutionary nature of international law forms the foundation of the incrementalist view that this body of law, with a few minor adjustments, can address the legal issues which arise with information operations. The notion of applying the contemporary law of armed conflict model to information operations causes some writers to assert a "maximalist" position[110] that the current legal paradigm cannot handle the new and complex legal issues inherent in information operations.[111] They argue that contemporary legal concepts based on agrarian and industrial age legal principles cannot adequately address

---

[108] ROGERS, *supra* note 106, at 2, *quoting* H. Lauterpacht, *The Problem of the Revision of the Law of War*, BRITISH YEARBOOK OF INTERNATIONAL LAW 382 (1952).

[109] Id., at 3.

[110] *See supra* note 24 and accompanying text.

[111] William T. Johnson, et al., *supra* note 24, at 4.

the cyberworld issues of use of force, territory, and sovereignty. Therefore, they assert that there should be a "third wave" legal paradigm to analyze "third wave" legal issues.[112] Thus, like someone wishing to discard an old, Springfield rifle for an automatic rifle because it appears to be new and "different" from the Springfield rifle, these writers apparently wish to discard the wisdom gained from centuries of experience in fleeting hope of embracing a new law of the next wave of warfare. Such a position is hasty and risky at this stage in our development of knowledge about information operations.

Before discussing the application of the current international law model to information operations, a review of the composition of international law is necessary. Such a review will provide the necessary knowledge and experience to appreciate the attempt to apply these rules to information operations which will follow it. Moreover, it will demonstrate that the paradigm upon which we currently rely, itself a product of evolution of ideas and concepts, can be further extended to information operations.

B. *International Law and Information Operations*

History is replete with examples of how technological changes influenced civilization to move forward.[113] International law has met the challenges presented by past innovations

---

[112] *See* Kanuck, *supra* note 6.

[113] Such examples include gunpowder, the use of the telegraph, railroad, and automobile to move ideas and resources more quickly, the development of the capability to have munitions delivered by mobile platforms such as tanks, submarines, and airplanes. Now we must look to see have how we will be able to collect, analyze, and disseminate information by computer technology.

in technology. The challenges presented by the technological innovations in information operations and warfare are no different. International law is applicable to these operations.

1. *The "Net Effect" Principle* – This principle I developed is a useful tool in applying a traditional legal framework to the new technological advancement in information operations and warfare. The net effect of warfare today is still the same: the subjugation of the enemy's will by force. With new technology, the subordination of the enemy 's will merely comes about quicker and more directly. Nevertheless, the result remains the same. Therefore, if the net effect of warfare is not altered by the use of newer technology, then the legal framework need not be discarded. For instance, if one state can attack and destroy another state with rifles or bows and arrows, what is the difference if it could do the same thing with tanks, submarines, aircraft or computers? What is the difference between State X sending its armed troops across the border into the sovereign territory of State Y in order to interfere in the sovereign affairs of State Y, and State X using the using computer technology to enter State Y's information infrastructure in order to interfere in its sovereign affairs? If one looks at the intended and the gained end results, the answer is that there really is nothing different except the means used to accomplish the mission. Based upon this net effect principle, once the net effect of an operation is understood, then the legal framework can be applied appropriately.

There are legal issues in information operations, particularly computer network-based operations, which challenge both the international and domestic legal models. For purposes of this thesis, only the international legal issues will be discussed. It should be noted that

these operations must also be considered in accordance with domestic laws of both the United States and any affected foreign territory.[114]

The net effect principle is composed of two parts:

a. *The Actor's Intent for the Intrusion* – The analysis of information operations under international law will rest upon determining a state's intention in using an information operations technique to enter another state's cyber-territory. Discovering the intended purpose of the information operation will assist in determining whether a state intended to interfere in the internal or international affairs of another state or whether it was a mistake. The answer concerning the actor's intention will determine what law will be applied and why a type of force may be used in response, if necessary. This thesis will focus only on whether an intrusion may constitute a use of force, aggression, or intervention into the affairs of another sovereign state under international law.

---

[114] It is extremely important to understand that there is no clear dividing line between information operations that fall within the purview of criminal law and those that fall within the realm of international law. These intrusions occur extremely quickly and, in many instances, anonymously. The inability to identify quickly and accurately the identity of an intruder and also ascertain the nature of their intrusion, poses a great challenge to government agencies. Only when these questions are answered, can the appropriate agency or department respond. Nevertheless, until that can occur, precious time is lost. Interview with Mr. M. E. "Spike" Bowman, Associate General Counsel, National Security Affairs, at Federal Bureau of Investigation, Washington, D.C. (Jan. 30, 1997); Interview with Special Agent Jim Christy, Senate Investigator (Congressional Fellow), at National Defense University, Ft. McNair, Washington D.C. (Mar. 4, 1997); Telephone interview with Martha Stansell-Gamm, Deputy Chief of Computer Crime and Intellectual Property Division, Department of Justice, on (Mar. 10, 1997).

b. *The Result of the Intrusion* – The other aspect of this analysis is to look at the result of the cyber intrusion into a state's cyber-territory. It will look at the nature of the intrusion into the state's sovereignty and the magnitude of the consequence of such intrusion. Thus, any state actor contemplating global engagement via the cyber superhighway must ensure that the nature of its activities does not constitute an intrusion on the sovereignty of another nation state. If such an intrusion occurs, it may be considered nothing at all or an act of intervention, aggression, or a use of force, depending upon the nature and magnitude of the result of the intrusion.

2. *Territory and Sovereignty of a State and Information Operations* -- Territory is one of the essential characteristics of nation states under the law of peace. When another state intrudes upon or interferes with the territory of another state, it ultimately threatens the sovereignty of the other state and destabilizes the peace among the community of nations. This destabilization could lead to further crisis or even armed conflict. Today, technology has enlarged the notion of territory. With the capability of signals and electromagnetic pulses to travel across international networks or through the atmosphere as radio waves, the opportunity to interfere and intervene in the affairs of other states is a reality.[115]

a. *The New Territory – cyber territory* -- Traditionally, the concept of territory extended only to those areas -- land territory and contiguous waters – that a state actually could control and were subject to its jurisdiction. Eventually, with the invention of

---

[115] *See* Stephen D. Bayer, *Comments: The Legal Aspects of TV Marti in Relation to the Law of Direct Broadcasting Satellites,* 41 EMORY L.J. 541 (1992) (hereinafter Bayer).

the airplane, the notion of territory expanded to include superjacent air space.[116] Additionally, if these areas could not be divided into sovereign territories, they were to be shared in common such as the sea and space.[117] Now the concept of territory based solely upon physical territorial and natural resources forming "geopolitical" borders in many instances, is extended by the intangible, spatial-political borders of cyber space.

These traditional notions of territory formed the foundation for the concept of the current battlefield – the air, land, and sea battlefield. This has now expanded to include "cyberspace."[118] What exactly is cyber space, however, is unclear, as it appears right now to be a territory with currently indefinable dimensions.[119] Unless we focus on analyzing information operations in terms of the actor's intent and result of the act on a state's sovereignty, we will be distracted by the issue of cyber territory.

---

[116] Most of the air law rules concern the aviation industry and many of these are found in international agreements such as the Warsaw Convention, which limits the liability of international air carrier. Convention for the Unification of Certain Rules relating to International Transportation by Air, 49 Stat. 3000, T.S. No. 876, 2 Bevans 983, 137 L.N.T.S. 11, October 12, 1929 (The Warsaw Convention). Another treaty is the Chicago Convention that establishes the rights of states over territorial airspace and civil aircraft. Convention on International Civil Aviation, Dec. 7, 1994, 61 Stat. 1180, 15 U.N.T.S. 295 [Chicago Convention] and the International Air Services Transit Agreement, 59 Stat. 1693, 3 Bevans 916, 84 U.N.T.S. 389, December 7, 1944 [hereinafter Chicago Agreement].

[117] United Nations Convention on the Law of the Sea, opened for signature Dec. 10, 1982, UN Doc. A/CONF.62/122 (1982); Treaty on Principles Governing the Activities of States in the Exploitation and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 UST 2410, 610 UNTS 205 [hereinafter Outer Space Treaty].

[118] *See* Philip Allot, *Note and Comment: Mare Nostrum: A New International Law of the Sea*, 86 AM. J. INT'L L. 764 (1992).

[119] *See supra* note 20 and accompanying text.

b. *Technology's Effect on the Concept of Territory* – The use of information systems raises several issues concerning this new aspect of territory. These issues focus on our current inability to identify the location of information in the system, the ownership of information, and the disruption of the systems or medium that convey the information. The maximalist approach looks at these issues and argues that the current paradigm cannot deal with these issues appropriately because of the undefined and intangible nature of the boundaries. However, the incrementalist looks at this situation and asserts that in time we will develop the capability to answer these questions more completely, but we cannot say that just because we have "imperfect" knowledge of information operations that the legal framework is unusable.

C. *Information Operations and the Spectrum of Operations: Peacetime, Crisis, and Armed Conflict*

Information operations can occur throughout the entire spectrum of military operations from peace to crisis to conflict and back to peace. The use of information and information systems is one of many capabilities within the US military element of national power which can support the national strategic engagement policy throughout the range of military operations. Such operations are effective throughout the spectrum of military operations to deter or defuse conflicts, promote democracy, or eliminate the need for military troops to enter a combat situation. As has been discussed throughout this section on international law, it is the net effect of the intrusion into the sovereignty of another state that

forms the foundation for review of these operations. This section will discuss offensive information operations using computer-network systems.

Currently, offensive information operations conducted during times of crisis are referred to as information warfare.[120] This means that even during peacetime, use of information operations in military operations other than war (MOOTW) which may involve a crisis of some nature – such as a humanitarian assistance mission or peacekeeping mission – are called information warfare. I suggest that another term, such as "information engagement operations," replace information warfare for use during these times prior to armed conflict and war. The term information warfare should be restricted to use during periods of armed conflict and war.

As our knowledge and terminology concerning information operations continues to undergo constant change, the use of terminology is particularly critical. The terms war and warfare have distinct meanings and corresponding implications under international law.[121] To use the term "warfare" in connection with information operations during non-warfare periods, including crisis in peacetime, is more than confusing; it is misleading and inaccurate. During peacetime, nations throughout the world constantly engage in efforts to influence

---

[120] JCS PUB. 3-13, *supra* note 5, at II-19.

[121] "State practice has emphasized that war is not a legal concept linked with objective phenomena such as large-scale hostilities between the armed forces of organized state entities but a legal status the existence of which depends on the intention of one or more of the states concerned." BARRY E. CARTER & PHILLIP R. TRIMBLE, INTERNATIONAL LAW 1286 (2d ed. 1995). War is a "hostile contention by means of armed forces, carried on between nations, states, or rulers, or between citizens in the same nation or state." Gitlow v. Kiely, 44 F.2d 227 (S.D.N.Y. 1930).

other nations, and they use multiple methods and means to accomplish their efforts. Although some nations are involved in "crisis" situations, these actions do not always amount to war or armed conflict unless such actions have the net effect of unabashedly intruding upon and intervening in the sovereign affairs of another state. Periods of crisis and conflict are not always periods of warfare.

Using the term "warfare" in connection with missions other than war also has a negative effect upon public perceptions of these operations. Due to the obvious interdependence of civilian and military information infrastructures, use of the term "warfare" in connection with information operations occurring on the information superhighway during periods other in than armed conflict or war can be unnerving.[122] The term information

---

[122] If the term warfare continued to be used during discussions regarding the information infrastructure or the "public internet," it would greatly disturb many Americans. They would recall the illegal efforts of the CIA and military to invade their privacy during the 1960s and 1970s. As the internet and other computer-based information systems touch the lives of so many Americans, using the term "warfare" in connection with this interdependent network may cause some Americans to think that the government might be waging war against them. *See generally* Senate Select Comm. To Study Government Operations With Respect to Intelligence Activities, Final Report of the Senate Select Comm. To Study Governmental Operations With Respect to Intelligence Activities, S. Rep. No. 755, 94th Cong., 2nd Sess., (1976) (generally termed the Church Committee) (investigated both foreign and domestic intelligence operations conducted by all government agencies and found, among other things, that the intelligence agencies during the 1960's and early 1970s: plotted to assassinate foreign leaders; participated in the overthrow of the government of Chile; opened private mail; read millions of private cables; infiltrated the news media and book publishing industry; and, even released propaganda to the American public.). Prior to the Church Committee's findings, the Rockefeller Commission, established on January 4, 1975 by President Gerald Ford and chaired by his Vice President, Nelson Rockefeller, investigated the Central Intelligence Agency after two newspaper articles reported that the CIA had engaged in widespread domestic spying. *See* Seymour Hersch, *Underground For the C.I.A. in New York: An Ex-Agent Tells of Spying on Students*, N.Y. TIMES, December 29, 1974, at A1; Seymour M. Hersch, *Huge CIA Operation Reported in U.S. Against Antiwar Forces*, N.Y. TIMES, December 29, 1974, at A1. The Rockefeller Commission reported back to the President that the CIA had exceeded its statutory authority and among other things,

warfare unnecessarily focuses upon the extreme end of the continuum of operations – armed conflict and warfare.

Offensive information operations employed during MOOTW should be called "information engagement operations." The term "information engagement operations" more accurately reflects the true purpose of these strategic information operations: to engage the global community on the information superhighway in order to deter and defuse conflict, reduce periods of conflict, and eliminate the necessity of employing military forces into a combat situation. In order to avoid confusion and to reflect the true intent of information operations during crisis, the term information warfare should be used strictly to refer to offensive information operations during armed conflict or war.

1. *Periods of Peace and Crisis* – During those periods short of armed conflict and war, the law of peace and the law of conflict management apply.[123] The domestic law of the United

---

conducted illegal mail searched, engaged in illegal wiretaps, and amassed vast amounts of information on lawful activities of U.S. citizens. *See* COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT (1975) (generally termed the Rockefeller Commission Report).

[123] *See* DEP'T OF ARMY, PAMPHLET 27-161-1, LAW OF PEACE, Vol. I 1-2 (September 1979) (hereinafter PAM 27-161-1) (The rules of conflict management provide a legal basis for nations to preserve and protect peace throughout the world. Essentially, nations, using legal principles to manage international conflicts, may use military forces with the purpose of eliminating or substantially reducing conflict within the community on nations. Such rules include rules on self-defense and intervention. While military forces may be engaged in activities other than armed conflict, the ultimate reality is that such forces may become engaged in armed conflict or war. The rules of hostilities encompass treaty provisions and other regulations applicable to armed conflict and the conduct of combat and resultant humanitarian operations. Although the nature of armed conflict and combat continue to change, customary international law and the extrapolations of such law based on experience, assist in bridging the gap with the codified international law, or when no codified law

States and other countries, various international agreements, treaties, and conventions, as well as customary law, apply to information operations involving computer-based networks and systems during these periods. By employing the net effect principle when analyzing these operations during these periods, and employing an incrementalist approach to the body of international law, it is clear that there is room to include these activities in the current legal framework.

In these operations, the intrusion into the sovereignty of another state is the issue. It must be determined if the intrusion amounted to a "use of force" or act of aggression both which are clearly prohibited under international law by the United Nations Charter. It may be determined that the intrusion was not a "use of force" or act of aggression, but rather another prohibited action, the "intervention" into the affairs of another sovereign which would only amount to, at best, a breach of contract.[124] Thus, knowing the net effect (intent and result) of the intrusion will assist in determining if the intrusion violated international law.

a. *Domestic Law* Considerations-- Although international law is the primary focus of this thesis, a complete discussion of the international law applicable to information operations must also include a discussion of any U.S. or foreign domestic law which may be

---

provision specifically addresses the issue, expanding current interpretations with the paradigm.).

[124] Not every intrusion by a state will amount to a violation of international law of armed conflict. These are instances where the act is not truly criminal in nature but still is an intrusion upon the sovereignty of the other state. The Doctrine of State Responsibility may apply in such situation. This doctrine states that one state is liable to another for reparations if it commits an act or an omission that is contrary to its obligations under international law. "Every breach of international law creates a duty to pay reparations for any loss or damaged caused."[124] Chorzow Factory (Ger. v. Pol.), 1928 P.C.I.J. (ser. A) No. 17.

applicable. A common example is espionage. Espionage is lawful under international law; however, it may be unlawful under the domestic law of a state.[125] An attorney must also review any stationing arrangements, Status of Forces Agreements (SOFAs), and also host nation laws to ascertain if there is any host nation domestic law which may govern information operations. This is critical research because SOFAs may restrict, prohibit, or even require advance notice of offensive information warfare activities launched from within the host nation. Host nation law may criminalize some information warfare activities, subjecting individual service member to potential prosecution.[126]

This review must also include a review of U.S. domestic laws and regulations regarding intelligence collection as part of the information operations.[127] Collection of

---

[125] During both international armed conflict and other times, espionage is not a crime under international law. *See* Convention (No. IV) Respecting the Laws and Customs of War on Land with Annex Regulations, Oct. 18, 1907, 36 Stat 2277, arts. 24 and 29-31 of the regulations for rules regulating the punishment of spies during an armed conflict. Such matters are strictly within the competency of the municipal laws of the victim state during peacetime.

[126] In addition to, or instead of espionage laws, some countries may also have computer crime laws under which conduct may be prosecuted. Of particulate note is the United Kingdom's Computer Misuse Act. This Act broadly proscribes many actions that would be included within the sniffing and cracking functions. Section 1(1), Computer Misuse Act 1990 provides: (1) A person is guilty of an offense if -- (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, (b) the access he intended to secure is unauthorized; and (c) he knows at the time when he causes the computer to perform the function that that is the case. Of even greater significance, however, is the fact that the Act purports to apply extraterritoriality, as long as any significant link with British jurisdiction. Computer Misuse Act, Section 4(2).

[127] National Security Act of 1947, 50 U.S.C. 401; Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801 – 1829; Title V of the National Security Act of 1980, 50 U.S.C. 413; Executive Order 12333, United States Intelligence Activities, December 4, 1981, 3 C.F.R. 200 (1982), 46 Fed. Reg. 59941, *reprinted in* 50 U.S.C. § 401; Executive Order 12863, President's Foreign Intelligence Advisory Board, September 13, 1993, 3 C.F.R. 632

information or intelligence is part of everyday operations. DoD is not prohibited from using overt means to collect intelligence on non-U.S. persons, or otherwise engage in those activities necessary to support traditional military intelligence or counterintelligence missions.[128] Covert actions, however, are viewed very differently, particularly with regards to the role of the military.[129] The statutes and policies indicate that in time of peace, the

---

(1993), 58 Fed. Reg. 48441, *reprinted in* 50 U.S.C. § 401; DEP'T OF DEF., DIRECTIVE 5240.1, DOD INTELLIGENCE ACTIVITIES (April 25, 1988); DEP'T OF DEF., REGULATION 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (December 7, 1982); DEP'T OF ARMY, REGULATION 381-10, U.S. ARMY INTELLIGENCE ACTIVITIES, 1 July 1984; DEP'T OF THE AIR FORCE, INSTRUCTION 200-19, CONDUCT OF INTELLIGENCE ACTIVITIES, October 1993; DEP'T OF THE AIR FORCE, INSTRUCTION 123-3, INTELLIGENCE OVERSIGHT, February 1985; DEP'T OF THE NAVY, SEC'Y OF NAVY INSTRUCTION (SECNAVINST) NO. 3829.3D AND 3820.3D, OVERSIGHT OF INTELLIGENCE ACTIVITIES WITHIN THE DEP'T OF THE NAVY, August 26, 1988; DEP'T OF ARMY, REGULATION 381-20, U.S. ARMY COUNTERINTELLIGENCE ACTIVITIES, 15 November 1993; DEP'T OF THE AIR FORCE, INSTRUCTION 124-11, AIR FORCE COUNTERINTELLIGENCE, October 1980; DEP'T OF THE NAVY, SEC'Y OF NAVY INSTRUCTION (SECNAVINST) NO. 3850.2. COUNTERINTELLIGENCE ACTIVITIES WITHIN THE DEP'T OF THE NAVY, August 26, 1988.

[128] DEP'T OF DEFENSE, DIR. 5240.1R, Procedure 2, authorizes DoD intelligence components to collect information on a United States person only (1) if the information is necessary to the conduct of a function assigned to that component; and (2) provided the information falls into one of the 13 authorized categories listed in Procedure 2.

[129] Covert action means an activity or activities of the U.S. Government to influence political, economic, or military conditions abroad where the role of the United States Government will not be apparent or acknowledged publicly. The Intelligence Oversight Act of 1980 (50 U.S.C. § 413b(e)). The Intelligence Authorization Act of 1991, Pub. L. No. 102-88, 105 Stat. 429 (1991) provides the same definitions as the Intelligence Oversight Act of 1980, however, what is excluded from this statutory definition are intelligence collection, traditional diplomatic and military activities, traditional law enforcement activities conducted by United States law enforcement agencies, traditional counter-intelligence activities, and routine support for all such activities. National Security Act of 1947 503(e), 50 U.S.C. 413b(e), as amended by Intelligence Authorization Act, Fiscal Year 1991, Pub. L. 102-88, 105 Stat. 429 (1991). This provides the basis for DoD to assert that certain operations are "traditional military activities" which do not require a Presidential finding. *See* John Broder & Melissa Healy, *Military Fights for Freer Role in Covert Operations*, L.A. TIMES, Apr. 6, 1990, at A1. DoD defines "covert operations" to be those "[o]perations which are so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. They

military is primarily intended to fulfill a role in support of the Central Intelligence Agency, and to a much more limited degree, the Federal Bureau of Investigation.[130] However, if either of the following two events occur, DoD may conduct special or covert activities:

- the nation is in a time of declared war, or a period of crisis requiring a Presidential report to Congress pursuant to the War Powers Resolution;[131] or
- a Presidential finding is made authorizing DoD to take covert actions intended to achieve a particular objective.[132]

Prior to authorizing any U.S. Government entity to engage in covert action, the President must submit a written finding to Congress[133] which details why:

- the action is necessary to support identifiable foreign policy objectives of the United States;[134]
- the action is important to the national security of the U.S.[135]

It is obvious that there is decentralized control over information warfare efforts concerning agencies charged with collection of material within their respective areas of

---

differ from clandestine operations in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation." JCS Pub. 1-02, at 95-96.

[130] E.O. 12333, Pt. 1.11(d).

[131] 87 Stat. 855.

[132] E.O. 12333, Pt. 1.8(e).

[133] 50 U.S.C. 413b(a)(1).

[134] 50 U.S.C. 413b(a).

[135] Id.

interest.[136] Control of covert foreign-focused information warfare efforts in peacetime rests with the CIA, with DoD in a supporting role. Within the U.S., the FBI controls information operations efforts, and DoD is in a (limited) support role. In almost every information operation category involving lawful covert action, DoD entities need a Presidential Finding to break out of their peacetime support role. Only during time of war, armed conflict, or declared national crisis does the military gain significant latitude to exploit covert information warfare capabilities.

b. *The International Law – the Unlawful Use of Force* – The acts of naked aggression which started World War II, and the atrocities which were committed during World War II lead to the creation of the United Nations Charter.[137] Based upon the collective experiences from World War II, the United Nations Charter Preamble states that it was established "to save succeeding generations from the scourge of war, which twice in our

---

[136] Although at present there is decentralized control over information warfare activities due to the lack of a national policy on the issue, all of the government agencies which are involved in intelligence matters share the same basic legal concerns, particularly concerning covert activities, in information warfare and operations. Much coordination occurs among this agencies. Interview with Dr. Kevin Powers, Assistance General Counsel (Operations), Office of General Counsel, National Security Agency, in Ft. Meade, Maryland (Jan. 31, 1997); Interview with Mr. Ben Crew, Analyst, National Imagery & Mapping Agency, at Defense Intelligence Agency Center, Bolling Air Force Base, Maryland, (Jan. 29, 1997); Interview with Mr. Gary Dean Baxter, Assistant General Counsel, Defense Intelligence Agency, Pentagon, Washington, D.C. (Jan. 31, 1997); Interview with Mr. George Jameson, Associate General Counsel, Central Intelligence Agency, in McLean, Virginia (Jan. 30, 1997); Interview with Mr. M. E. "Spike" Bowman, Associate General Counsel, National Security Affairs, Federal Bureau of Investigation, Washington, D.C. (Jan. 30, 1997); Interview with Mr. Thomas J. Benjamin, Associate General Counsel, Directorate of Science and Technology, Central Intel. Agency, McLean, Virginia (Jan. 30, 1997); Interview with Mr. William Harvey Dalton, Associate Deputy General Counsel, International Affairs & Intelligence, Office of the General Counsel, Department of Defense, in Pentagon, Washington, D.C. (Jan. 30, 1997).

lifetime has brought untold sorrow to mankind."[138] The document further set forth in Article 1 that "[t]he purposes of the United Nations are to maintain international peace and security and to that end: to take effective collective measures for the prevention and removal of threats to the peace . . . ."[139] The Charter provides in Article 2(3) that "All members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered." To ensure that its established purposes to preserve and maintain peace throughout the world, the drafters of the Charter created the Security Council to enforce the Charter.[140] Its creation was based upon the previous failures of the League of Nations[141] and the Kellog-Briand Pact.[142]

(1) *The Use of Force* – Beginning in the late nineteenth century, nations began attempting to limit war, prompted by the advent of mass armies and the continual growth in the efficiency of weapon systems.[143] The focus quickly became renouncing not all war, but aggressive war. The culmination of this effort was the Kellog-Briand Pact of

---

[137] U.N. CHARTER, Jun. 26, 1945, 59 Stat. 1031, 24 U.N.T.S. 2225 [hereinafter UN Charter].

[138] Id., at pmbl.

[139] Id., art. 1, para. 1.

[140] The UN Charter created the Security Council and its authority and responsibilities in several articles of the Charter – Arts. 24, 25, 33, 34, 36, 37, 39, 41, 42, 43.

[141] Id., at pmbl, art. 1., para. 3; Covenant of the League of Nations (1919).

[142] Treaty Providing for the Renunciation of War as an Instrument of National Policy, Aug. 27, 1928, 46 Stat. 2343, U.N.T.S. 57 (also known as the Kellogg-Briand Pact).

[143] VON GLAHN, *supra* note 108, at 670.

1928.[144] The difficulty was creating a mechanism to enforce this renunciation. Following World War II and the failure of the League of Nations, the United Nations became that mechanism and incorporated and expanded on many ideas about limiting war within its Charter. This remains the situation today. Thus, there are now two types of force – defensive and aggressive. The first is permissible and is discussed in Section below, the other has been asserted since the War Crimes tribunals at Nuremberg to be illegal.[145] The focus, then, in conflict is the concept of aggression.

The difficulties with this concept are several. The first and most fundamental is that no one really agrees on what the term aggression means,[146] at least in the sense of enforceably prohibiting certain conduct. Second, the UN Charter provision preserving the right of self-defense[147] is interpreted by many nations (including the United States) as allowing anticipatory self-defense.[148] Other nations view this type of anticipatory attack as

---

[144] *See supra* note 146 and accompanying text.

[145] International Military Tribunal (Nuremberg) Judgment and Sentences, 43 AM. J. INT'L L. 168 (1949) ("To initiate a war of aggression, therefore, is not only an international crime; it is the supreme international crime differing only from other war crimes in that it contains within itself the accumulated evil of the whole."). Specifically, the Nuremberg Tribunal's charter defined "planning, preparation, initiation or waging of a war of aggression" a crime against peace." CHARTER OF THE INTERNATIONAL MILITARY TRIBUNAL, Oct. 6, 1945, 59 Stat. 1546.

[146] VON GLAHN, *supra* note 108, at 676. "Until now, the present writer believes, no generally binding definition of what is meant by aggression has come into being, despite the General Assembly's approval of its Special Committees definition . . . .").

[147] UN CHARTER, at art. 51.

[148] Anticipatory self-defense is a concept "[u]nder existing customary international law, [whereby] states do not always have to wait until after an attack has been absorbed to undertake self-defense. Rather, where the threat is sufficiently imminent in point of time, they can chose to strike first, providing, of course, that the strike is within the parameters of

aggression. Finally, the United Nations Charter authorizes the use of force by the security council to "restore international peace and security"[149] if the Council determines "the existence of . . . [an] act of aggression . . . ."[150] Thus, the meaning of aggression is critical.

To assist in the Security Council's efforts, the UN General Assembly adopted a definition of aggression.[151] It defines aggression generally as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this definition."[152] The resolution goes on to list a number of acts that serve as prima facie evidence of aggression including such things as invasion, bombardment, and blockade.[153] Article 4 quickly goes on to add, however, that this list is not exhaustive.[154] Further, Article 6 states that the definition should not be construed "as in any way enlarging or diminishing the scope of the Charter, including its provisions concerning cases in which the use of force is lawful."[155] This preserves the concept of self-defense, including the controversy over

---

discrimination, proportionality, and military necessity." Louis Rene Beres, *The Legal Meaning of Terrorism for the Military Commander,* 11 CONN. J. INT'L L. 1, 12-13 (1995).

[149] UN CHARTER, *supra* note 138, at art. 42.

[150] Id.

[151] Definition of Aggression, U.N.G.A. Res. 3314 (XXIX) (1975). *See infra* note , and accompanying text.

[152] Id., at art. 1.

[153] Id., at art. 3.

[154] Id., at art. 4. ("The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter.").

[155] Id., at art. 6.

anticipatory self-defense. Still another problem with this definition, is that it does not address the situation where the use of force is not conducted by a state. Most important when considering this definition, however, is that it is merely guidance.[156] It is not a binding rule, but was essentially put forward to help the Security Council in its role determining the existence of an act of aggression pursuant to the Charter.[157]

(a) *Information Operations as Aggression* – The coming wave of information is sure to change this concept of aggression. The UN definition at least reflects the consensus of nations as to the type of things that can constitute aggression. One of these is the use of armed force against the political independence of another state.[158] Surely, it will not be long before the use of information assets will be considered the use of information weapons, particularly when used to influence the political posture of another nation. In fact, considering the use of information has been found to be an integral part of waging a war of aggression.

---

[156] The resolution "recommends that [the Security Council] should, as appropriate, take account of that Definition as guidance in determining, in accordance with the Charter, the existence of an act of aggression." Id., at item 4.

[157] Professor von Glahn asserts that the definition is not biding and states that "[I]t should be kept in mind that General Assembly resolutions do not create obligatory rules of international law." VON GLAHN, *supra* note 108, at 676-78. Others, however, disagree, since the definition "is the most recent and most widely (albeit not universally) accepted." YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 120-21 (1988). As such, it is at least arguably customary international law. In fact, "[a]t least one paragraph of the definition, namely, Article 3(g) . . . has been held by the International Court of Justice, in the Nicaragua case of 1986, to mirror customary international law." Id., at 121, citing *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Merits)*, 1986 I.C.J. 14, 103. Article 3(g) is part of the listed acts of aggression in the UN Definition. It prohibits the "sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State . . . ."

The trial at Nuremberg demonstrated that the Nazi propaganda machine was one of the most powerful weapons in the German arsenal. It was this "weapon" that promoted the actions of the Nazis. Consequently, the use of propaganda was considered part of the conspiracy to plan, prepare, and conduct a war of aggression.[159]

(b) *Information Operations as Ideological Aggression* -- Additionally, during the debate leading up to the UN Definition of Aggression, a concept surfaced that extends aggression to include information acts. This concept was labeled "ideological aggression." While there was insufficient support to include this idea in the UN definition,[160] there is at least a good faith basis for including it in a charge of a violation of international law based on precedent before international organizations.[161]

---

[158] Definition of Aggression, *supra* note 152, at art. 1.

[159] *See* I TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL 30-31, 293-94 (1947) (discussing propaganda as one of the "opportunistic methods" used by the Nazi conspirators and the indictment of Rosenberg as the party "ideologists"). Additionally, the advocating of the so-called "final solution" was considered part and parcel of "crimes against humanity" when considering the crimes of Streicher. *See* Id., at 302. In some instances, it appears that the tribunal did not consider propaganda alone to be enough for conviction. *See* Id., at 336-38 (acquitting Herr Fritzsche, finding that although he "made strong statements of a propagandistic nature in his broadcasts[,] the Tribunal is not prepared to hold that they were intended to incite the German people to commit atrocities . . . .").

[160] *See* VON GLAHN, *supra* note 108, at 677 ("[N]o agreement was achieved on whether any definition of aggression ought not to include what might be termed indirect aggression, such as conspiracies organized abroad or ideological propaganda."; JULIUS STONE, AGGRESSION AND WORLD ORDER 59-60 (1987) (discussing the disagreements over ideological aggression during some of the earlier discussion in the 1950s and 1960s that led eventually to the UN definition.).

[161] *See* THOMAS & THOMAS, *infra* note 272, at 85-88 (discussing a number of complaints made to a variety of international organizations based upon hostile propaganda.).

There is no generally accepted definition of ideological aggression. However, those who do define it tend to define it in terms of the means by which you obtain its generally accepted object, that is "the actual or intended imposition of an ideology."[162] Given the definition of ideology discussed previously and the influence of perception on it, the methods considered aggressive in this concept are those that are "adapted to the molding of the thought processes of the people of a state so as to maintain the condition of things in the state intact or to effect change in the condition of things in that state so as to accord with the aggressor's wishes."[163] Ideological aggression then "is the spreading of ideas intentionally and deliberately so as to manipulate by symbols controversial attitudes and positions."[164]

In this classical sense of ideological aggression, there were considered three types of propaganda that fell within the definition. The first is war-mongering propaganda which essentially was urging the other state to be the first to commit an act of war by declaration,

---

[162] Id., at 83. Propaganda has been defined as a "systematic attempt through mass communications to influence . . . thinking and . . . behavior . . . ." LESLIE JOHN MARTIN, INTERNATIONAL PROPAGANDA: ITS LEGAL AND DIPLOMATIC CONTROL 12 (1958). The U.N. Committee on the Peaceful Uses of Outer Space (COPUOS) describes propaganda as "a hostile act, broadcasts of which may provoke war, incite subversive activities, slander receiver countries, interfere with receiver's internal affairs, and violate human rights." U.N. GAOR Committee on the Peaceful Uses of Outer Space, 25th Sess., at 7, U.N. Doc. A/AC.105/79 (1970). The COPUOS is a General Assembly committee formed in 1959 to address a variety of technical and security-related issues. RITA LAURIA WHITE & HAROLD M. WHITE, THE LAW AND REGULATION OF INTERNATIONAL SPACE COMMUNICATION 236-37 (1988).

[163] Id., at 83-84.

[164] Id., at 84.

invasion, blockade, etc.[165] The second is subversive propaganda which is the advocating of civil strife or war within the other state.[166] The third is defamatory propaganda which is "directed against the leaders of the government of the state."[167]

The effects of the Information Age can only serve to expand this definition. As the disparity of knowledge grows between the Third Wave societies and those that remain in the First and Second Waves, the Third Wave societies will be increasingly able to powerfully influence actions in the First and Second wave societies without using "armed force" in the classical sense.[168] This will cause an outcry among the societies being influence.

---

[165] THOMAS & THOMAS, *supra* note 272, at 84.

[166] Id.

[167] Id., at 85. The authors assert that "[d]efamatory propaganda violates customary international law." Id. citing J. WHITTON & A. LARSON, PROPAGANDA: TOWARDS A DISARMAMENT IN THE WAR OF WORDS 56 (1963).

[168] *See* Bayer, *supra* note 116, at 541-42 ("Advances in Communications technology have enabled television broadcasts to transcend state boundaries and send signals directly to the viewer. TV Marti is a United States government-sponsored television project that has been broadcasting news, information, and entertainment directly to Cuban households since March 1990. Voice of America broadcasts TV Marti from a transmitter and antenna in a balloon tethered 10,000 feet above the ground in the Florida Keys, only ninety miles from Cuba. TV Marti's transmission is similar to that of short-wave radio and beams into Cuba on Cuban television's channel thirteen. The television signal bypasses all ground retranslation stations and cable companies; therefore, the Cuban government cannot directly control the TV Marti signal before it reaches individual Cuban viewers. Although it utilizes unique technology, the communication concept of broadcasting directly to a viewer without government intervention is not new. The direct broadcasting satellite, or DBS, has been around for almost two decades and, like TV Marti, enables broadcasts from a around the world to reach individual television sets; however, the viewer must have a parabolic antenna, or satellite dish, to receive these broadcasts. Developed nations continue to grapple with the immense potential of the direct broadcasting satellite. The issues of propaganda, international regulation, and interference compromise the ongoing controversies over the DBS system and manifest themselves once again in the TV Marti debate."). *See also* THOMAS L. MCPHAIL, ELECTRONIC COLONIALISM: THE FUTURE OF INTERNATIONAL BROADCASTING AND COMMUNICATION 181 (1981) (hereinafter MCPHAIL)J; MARIKA N. TAISHOFF, STATE

Consequently, the concept of ideological aggression is likely to expand and become generally accepted as a necessary means for the international establishment to try to make fact their goal of sovereign equality among nations, even though this equality does not really exist today.

The implications are that a nation must employ information operations carefully. Technological capabilities will allow Third Wave societies, like the U.S., to influence things in other nations more readily than even before. Regardless of motive, the recipient of these acts could consider them aggressive acts.[169] Characterizing actions as aggression could give rise to problems in the legal and political realms of the international community ranging from condemnation to conflict.

RESPONSIBILITY AND THE DIRECT BROADCAST SATELLITE 30-51 (1987) (Both McPhail and Taishoff demonstrate that DBS transmissions may be either intentional or unintentional by spilling over the border into a receiving country, however, many countries are deeply concerned about the free flow of information because of the tremendous possibilities for propaganda, threats to national sovereignty, commercialism, and harm to their cultural interests.). *See* Emil Konstantinov, *Definition, Characteristic Features and Impact of International Direct Television Broadcasting, in* 1988 PROCEEDINGS OF THE 31ST COLLOQUIUM ON THE LAW OF OUTER SPACE 295 (1988) (since only industrialized nations such as the United States, Japan, Canada, and EEC nations possess the capability to use DBS broadcasts systems. Thus, this enables the industrialized nations to broadcast communications that reflect their ideas and cultures at the expense of countries with less advanced communications systems.). In short, a DBS television broadcast is "[a] radiocommunication service in which signals transmitted or retransmitted by space stations are intended for direct reception by the general public." 47 CFR ch.1 (10-1-89 Edition), FED. COM. COMM. 55586, §100.3.

[169] *See* Bayer, *supra* note *116,* at 547-48 (1992) ("Countries that fear DBS technology and its ramifications base their legal argument on the concept of state sovereignty . . . . However, counties which receive unwanted communications via radio or television insist that a line be drawn to protect against propaganda.").

(c) *Article 2(4) of the U.N. Charter* -- This article provides that "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity and political independence of any state, or in any other manner inconsistent with the Purposes of the U.N." The word "force" is not defined anywhere within the U.N. Charter. Unfortunately, force does not have a fixed meaning. "Its meaning comprises – strength, energy, power, intense effort, and influence, vitality of [an] army to use violence, to violate, to exhort, to compel."[170] Prior to the development of international institutions like the League of Nations and the United Nations, "the term force had been applied in the context of war or hostilities in its many forms and extensive scale between states. In practice of states, use of force was identified with war."[171]

There has been a great deal of controversy over the meaning of Article 2(4) since 1945, with recent controversy arising as a result of scientific developments. As the means of communication advances, the interdependence of nations upon each other in economic and other fields grows at a rapid pace, and the disparity among the economically developed and under-developed states increases, a number of states started to recognize that if the United Nations adopted an expansive view of Article 2(4) they would be in danger.[172] They believed that they were at more risk from economic and other types of coercion than any "armed" use of force. Therefore, they have pushed to keep a restrictive interpretation of "use

---

[170] SUBHAS C. KHARE, USE OF FORCE UNDER U.N. CHARTER 7 (1985) [hereinafter KHARE].

[171] Id.

[172] Id.

of force" under Article 2(4),[173] one focusing solely upon "armed" force. Therefore two views developed about the meaning of the word "force" as used in the Charter. The restrictive view holds that "force" means armed or physical force. The other view, the liberal view, asserts that force means not only physical or armed force, but also other manifestations of coercion such as economic coercion. Those that support this view base their argument on grounds other than a legal one. They "contend that the interpretation of the Charter should not merely conform to the letter and spirit of the Charter, but should reflect the current needs of the members of the United Nations.[174]

While the restrictive view of the use of force predominated interpretations during the last few decades, the use of information operations is prompting a call for the adoption of the liberal view. This allows for a more refined understanding of the word "force" based upon the experiences of the last fifty years. The physical attributes of force have changed since the creation of the United Nations, however, the law is slower to recognize this fact. The liberal view, like an incrementalist approach, would modify slightly the current paradigm to include a United Nations answer regarding the legal issue of use of force and information operations.[175]

---

[173] Id., at 7-8.

[174] Id., at 8

[175] Commander James M. Bond, Peacetime Foreign Data Manipulation as One Aspect of offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4) (1996) (unpublished manuscript) (on file with author), at 46 [hereinafter Bond].

Application of the net effect principle to intrusions will enable one to determine if the intrusion amounts to a prohibited use of force even if there is no acceptance of an expansive view of the concept of force. Clearly, if an operation would yield a net effect that would be a violation of the Charter, then any other act which would render the same net effect logically should be a violation also. For example, if taking a tank battalion across the border into another country to accomplish a military objective is a violation of the Charter, then why is one country's intrusion into another country's domain, through the information system to accomplish a military mission with a similar end result, not considered a use of force? By analogy and logic, there must be other acts of coercion that are equivalent to physical coercion depicted in the Charter.[176]

It is the net effect principle that corresponds to the arguments of some writers who assert that the use of force would include "an exercise of power in the territorial domain, but no use of arms."[177] Therefore, in those instances where the effect of the information operations is as devastating as the application of conventional operations, it is only a natural and evolutionary step to conclude such operations are the equivalent of an armed attack.

---

[176] In Nicaragua v. U.S. (1986 ICJ 4) (the International Court of Justice ruled that the provision of arms by Nicaragua to the leftist rebels in El Salvador did not constitute an armed attack on El Salvador, so it could not form the basis of a collective self-defense argument that would justify the laying of mines in Nicaraguan waters or certain attacks on Nicaraguan ports, oil installations and a naval base – acts that were imputable to the United States. The Court said it had sufficient evidence to determine whether certain cross-border incursions by Nicaraguan military forces into the territory of Honduras and Costa Rica constituted armed attack.. Economic sanctions such as embargoes have not been held to be attacks.)

[177] IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE 362 (1963) (hereinafter BROWNLIE).

Thus, accepting this definition entails the application by analogy of the traditional customary and convention-based precedents.[178]

---

[178] As discussed above, *see supra* note 152, and accompanying text, outside of the UN Charter, the General Assembly attempted to define aggression as "the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another state, or in any manner inconsistent with the [UN]Charter . . . . important terms: armed force, sovereignty, territorial integrity, and political independence." Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc. A/9631 (1975). The resolution provides that a "first use of armed force" by a State in contravention of the Charter is prima facie evidence of act of aggression. Additionally, Article 3 of this Resolution provides a list of seven acts that qualify as aggression. All these actions involve the use of physical force and armed forces. Article 3 of UN General Assembly Resolution 3314 lists the following seven acts, regardless of a declaration of war, as acts of aggression:

1. Invasions or attack by the armed forces of a State of the territory of another State, or any military occupation, however, temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;

2. Bombardment by the armed forces of a State against the territory of another State or the use of any weapon by a State against the territory of another State;

3. The blockage of the ports or coasts of a State by the armed forces of another State;

4. An attack by the armed forces of a State on the land, sea, or air forces, or marine and air fleets of another State;

5. The use of armed force of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement of any extension of their presence in such territory beyond the termination of the agreement;

6. The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;

7. The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein. Id., at art. 3.

What is important is Article 4 of this Resolution states that the "acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter." Id., art. 4. Thus, between the language in the latter half of Article 2(4) and the recognition in the U.N. Resolution of a non-exhaustive list

(d) *Article 2(7) of the UN Charter* – The principle of non-interference or non-intervention is embodied in Article 2(7) of the UN Charter.[179] Like other Charter provisions such as Article 2(4) and the term "use of force," and Article 51's term "self-defense", this Article also has vague terminology in it.[180] However, it is clear that the United

---

of aggressive acts, there is sufficient substantiation that opportunities exists for the U.N. Charter to embrace certain information operations as use of force or aggression. *See also* Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N. Doc. A/8028 (1970). This Declaration reaffirms the UN Charter prohibition against aggression; the duties of states under the Charter and customary international law in regard to: the duty not to use the threat or use of force against states; the duty to settle disputes peacefully; the duty not to intervene in domestic matters; duty to cooperate; duty to ensure equal rights and self-determination of peoples; the duty to preserve sovereign equality of states; and the duty to fulfill in good faith obligations under the Charter.

[179] Article 2(7) of the UN Charter provides that "[n]othing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII." (emphasis added). UN Charter, *supra* note 138, at art. 2(7).

[180] Contemporary practice demonstrates that the phrase "essentially within the domestic jurisdiction" has moved beyond has the restraint of complete noninterference to allow several grounds for "justifying multilateral protection of democracy. For example, where a denial of democracy is effected by violent repression, state practice indicates that there is a right of intervention based on humanitarian imperatives and the right to self-defense of the people. The United States intervention in Haiti stands as a prominent example." Reginald Ezetah, *The Right to Democracy: A Qualitative Inquiry,* 22 BROOKLYN J. INT'L L. 495, 508 (1997) (footnotes omitted). *See also* Michael Byers, *Custom, Power, and the Power of Rules Customary International Law From An Interdisciplinary Perspective,* 17 MICH. J. INT'L L. 109, 180 n.245 (1995) ("An example of this phenomenon might be the recent expansion of the 'right' to humanitarian intervention. Article 2(7) of the U.N. Charter prohibits intervention except in situations where, in terms of Chapter VII, there is a threat to or breach of international peace and security. The situations in northern Iraq, Somalia, Haiti, and Rwanda, with the possible exception of the problem of refugees, do not seem to fall within this context as it is traditionally been understood. However, instead of changing the rule, or creating a new rule to allow intervention for humanitarian purposes in situations not threatening to international peace and security, the international community has chosen to

Nations does not condone the intervention in the internal affairs of nations,[181] unless there is a threat to "international peace and security" which would permit the Security Council to call the system of collective security established in Chapter VII.[182]

2. *The Authorized Uses of Force* – There are two basic areas where the use of force is authorized. The first includes actions in self-defense in accordance with Article 51 of the U.N. Charter, and the second includes actions employing the use of force when sanctioned by the Security Council.

---

view these an unique situations justifying ad hoc enlargements of the international peace and security concept. In short, the international community's interpretation of Chapter VII has arguably been modified without the text of the Charter having been changed."). *Cf.* Michael J. Glennon, *Sovereignty and Community After Haiti: Rethinking the Collective Use of Force,* 89 AM. J. INT'L L. 70, 71-72 (1995).

[181] *See* Anthony F. Perez, *On the Way to the Forum: The Reconstruction of Article 2(7) and rise of Federalism Under the United Nations Charter,* 31 TEX. INT'L L.J. 353, 359 (1996) (hereinafter Perez) (The nineteenth century "classical view [of nonintervention] reflected a broad tolerance for intervention, one in keeping with the ruling ideology of balance of power and the realities of the hierarchical distribution of power in the international system of the period . . . . [T]he classical doctrine served nonetheless as the springboard for a more precise and restrictive doctrine of nonintervention . . . ." developed during the twentieth century.).

[182] *See* L.C. Green, *Command Responsibility in International Humanitarian Law,* 5 TRANSNAT'L L. & CONTEMP. PROBS. 319, 344 (1995) ("This [does] not mean that there were not instances, as in post-1945 Greece, when some powers argued that revolutionary forces were the surrogate for some rival greater power whose expansionist influence had to be countered. Nevertheless, the United Nations Charter supported the general principle, only modifying if to the extent that U.N. action was permitted, if there was a threat to the maintenance of international peace and security."). Although some writers indicate that there has been an evolution of the practice and notion of the noninterference principle in favor of pro-democracy intervention, some writers assert that the principle of noninterference has become an important counterweight to a Western-dominated new world order for "less developed countries, non-aligned nations and surviving socialist states" . . . who are no longer able to "manipulate the politics of a bipolar world" but desire to limit the "Security Council's action under the Western-dominated new world order." Douglas Lee Donoho, *Evolution or Expediency: The United Nations Response to the Disruption of Democracy,* 29 CORNELL INT'L L.J. 329, 372-73 (1996).

(a) *Use of Force Sanctioned by the Security Council* -- The United Nations Security Council can authorize the use of force to restore international peace and security in accordance with Chapter VII of the U.N. Charter.[183] Under Chapter VII, the UN Security Council may authorize "all necessary means" by its member states to restore international peace and security."[184] Such Security Council authorizations have included authorizing peace enforcement actions to defuse and reduce internal conflicts the former Yugoslavia, Haiti, Somalia, and Iraq.[185]

(b) *Article 51 Self-Defense* – Article 51 of the U.N. Charter provides that "[n]othing in this present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and

---

[183] UN Charter, *supra* note *138, at* art. 39.

[184] Id. Chapter VII of the UN Charter provides for various measures in enforcement actions. "Measures" under Article 41 relates to "measures not involving the use of armed force" includes many aspects of information operations, and under Article 42, the measures involve the use of armed force. These are also the enforcement measures contemplated under Article 2(7) concerning nonintervention. *See* Perez, *supra* note 182, at 362.

[185] See S.C. Res. 1031, U.N. SCOR, 50th Sess., 3607th mtg. at 3, U.N. Doc. S/RES/1031 (1995) (authorizing use of "all necessary measures" in the former Yugoslavia to ensure compliance with Dayton Accords); S.C. Res. 940, U.N. SCOR, 49th Sess., 3413th mtg. at 2, U.N. Doc. S/RES/940 (1994) (authorizing intervention in Haiti); S.C. Res. 794, U.N. SCOR, 47th Sess., 3145th mtg. at 3, U.N. Doc. S/RES/794 (1992) (authorizing intervention in Somalia); S.C. Res. 688, U.N. SCOR, 46th Sess., 2982d mtg. at 2, U.N. Doc. S/RES/688 (1991) (condemning Iraqi repression of Kurds). *See also* Michael J. Glennon, *Sovereignty and Community After Haiti: Rethinking the Collective Use of Force*, 89 AM. J. INT'L L. 70 (1995); Ruth E. Gordon, *Intervention by the United States: Iraq, Somalia, & Haiti*, 31 TEX. INT'L L.J. 43 (1996).

security."[186] For purposes of this thesis, the focus of concern is what act of intrusion by a State amounts to an "armed attack" to warrant a legitimate claim under Article 51. While "armed attack" under Chapter 51 and "use of force" under Article 2(4) are not the same, these terms are similar in that they point to some sort of uninvited and unauthorized entry or intrusion into the affairs of one state by another. There has been an on-going struggle to expand incrementally the meanings of these two terms from their traditional focus on armed military force.[187]

Employing the net effect principle to both the intrusion and the response provides an analogous basis upon which to justify measures taken in self-defense. For example, what if State X intrudes into State Y's information infrastructure and launches a computer-based system offensive information operation which has the net effect of disrupting and partially destroying State Y's primary power grid, as well as its communications and financial systems and ultimately causing thousands of civilian deaths? If State Y ascertained, with certainty, that State X actually launched the attack and that it was not a mistake, one would have a difficult time arguing that just because State X's intrusion into State Y did not technically fall within the U.N. Charter's current definition of use of force, State X's was not a clear violation of State Y's sovereignty. Logically, State Y, out of necessity to protect its sovereignty, should be able to respond quickly, with proportional force of its own.

---

[186] UN Charter, *supra* note 138, at art. 51.

[187] *See generally* Bond, *supra* note 176.

Moreover, if State Y learned that State X was going to employ this offensive information operation, would State Y have to wait until the "attack" or intrusion occurred before it could take defensive actions? In essence, must a nation wait to take the first hit before it can defend itself? The answer is no. State Y does not have to wait for the attack whether the attack is with conventional weapons or information operations measures. However, State Y must be able to demonstrate that the attacker possessed the capability to proceed with the attack and the attack was imminent.[188]

Just as there are conflicting views regarding the meaning of "force" in Article 2(4), there are also two views on when a state may employ a self-defense measure. There is a very restrictive minority view which hold that the U.N. Charter has preserved the customary right of self-defense under Article 51.[189] Nevertheless, it asserts that at the same time it limited to

---

[188] For discussion of self-defense, and particularly the elements of anticipatory self-defense, *see supra* note 149 and accompanying text.

[189] The contemporary concept of self-defense is rooted in both customary and codified international law. Self-defense has been regarded as an instance of self-preservation. In 1842, Secretary of State Daniel Webster, attempted to describe the limits on the notion of self-defense in a letter to Lord Ashburton of the British Government, by having the British, with regard to their actions taken against *The Caroline*, show the existence of "necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation. It will be for it to show, also, that the local authorities of Canada, even supposing the necessity of them moment authorized them to enter the territories of the United States at all, did nothing unreasonable or excessive; since the act justified by the necessity of self-defense, must be limited by that necessity, and kept clearly within it." BROWNLIE, *supra* note 178, at 43. Thus, the right of self-defense, specifically the claim of anticipatory self-defense, is stated in terms of the tests laid down by Webster in the correspondence relating to the *Caroline* incident. Therefore, a claim of anticipatory self-defense must meet three specific criteria: (1) the threat in issue must be imminent/immediate; (2) the action taken must be necessary (no viable alternative); and (3) the force used must be proportionate to the threat posed. Article 51 of the United Nations provides that "[n]othing in the present Chapter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the UN until the Security Council has taken measures necessary

the extent of response specified in Article 51. Therefore, a member only has the right to respond in self-defense when an armed attack has occurs. Like the restrictive view regarding Article 2(4), this is also a restrictive view regarding Article 51 -- if the language of the Charter states an armed attack, then it must be an armed attack.[190]

On the other hand, the liberal view on when self-defense measures may be executed, which is now more widely accepted, contends that Article 51 in no way circumscribes the customary right of self-defense. Thus, a state can act in self-defense not only in a case of an armed attack, but also in instances against the threat of imminent attack to defend and safeguard other rights.[191] There is no indication that inclusion of the words "armed attack" in Article 51 was intended to prevent the use of force in meeting unlawful and unauthorized forcible acts in instances other than an armed attack.[192]

---

to maintain international peace and security . . . ." Some nations take the view that the customary law right of self-defense to repel imminent armed attacks and not just actual armed attacks, is much broader that the self-defense concept found in Article 51 of the UN Charter which specifically references "if an armed attack occurs." Many other nations, including the United States, assert that the inherent right of self-defense, including the concept of anticipatory self-defense, still exists. This position is based on the argument that the inherent right of sovereign nations to defend themselves was never negotiated away in the UN Charter. *See* Robertson, *supra* note 107, at 103. *See also* Morgan, *supra* note 6, at 307-08.

[190] *See supra* note 174 and accompanying text.

[191] KHARE, *supra* note 171, at 85.

[192] Id.

(3) *Actions equating to less than force may still violate international law* -- In the Corfu Channel Case,[193] the International Court of Justice[194] found that Britain violated international law by intruding into Albanian waters with military force, even though it did not constitute an armed attack.[195] Respect for territorial sovereignty is an essential foundation of international relations Between independent states. The "Declaration on Inadmissibility of Intervention into the Domestic Affairs of States,"[196] offers an additional perspective on impermissible intervention. Paragraph i. of the Declaration provides that "[n]o State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its

---

[193] Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 28 (under customary international law, the International Court of Justice held that ships of all nations have the right to navigate "through straits used for international navigation between two parts of the high seas without the previous authorization of a coastal State," including warships in time of peace, "provided that such passage is innocent.").

[194] The International Court of Justice (ICJ) is the successor to the Permanent Court of International Justice (PCIJ), which was established in 1920 under the auspices of the League of Nations. The ICJ, the principal judicial organ of the United Nations, came into existence in 1945. Its Statute or constitution, Statute of the International Court of Justice, (June 26, 1945, 59 Stat. 1055, T.S. No. 993, 3 Bevans 1179) modeled on that of the PCIJ, is annexed to and forms an integral part of the United Nations Charter. All Member States of the United Nations are automatically parties to the Statute (U.N. Charter, Art. 93).

[195] The International court of Justice held that the British violated international law with its intrusion into Albanian waters for the purpose of testing the Albanian government, but this act by the British did not constitute and armed attack. Id. at 34-35. This decision leads one to the conclusion that armed attacks are a use of force, but not all uses of force are equivalent to armed attacks. "All uses of force in violation of 2(4) are not armed attacks allowing a state to respond with force under the guise of Article 51." *See* Bond, *supra* note 176, at 63-64.

[196] Declaration on the Inadmissibility of Intervention in the Domestic Aff. of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131, U.N. GAOR, 20th Sess., Supp. U.N. Doc. A/2131/Rev. 1 (1966).

political, economic and cultural elements are condemned." Paragraph v. of the Declaration states that "[e]very State has an inalienable right to choose its political, economic, social, and cultural systems, without interference in any form by another State."[197] This declaration clearly focuses upon the net effect of a state's action with respect to another state and how that action intrudes upon the essence of the nation state.

The Chorzow Factory Decision[198] focuses upon the "doctrine of state responsibility" with respect to a state's breach of a legal responsibility under international law. The "doctrine of state responsibility" provides that every breach of international law creates a duty to pay reparations for any loss or damage caused.[199] This is critical to consider when analyzing offensive information operations in the peace and crisis realm of the spectrum of operations. Unlike instances of armed conflict when damage caused by combatants is "excused," damage caused outside of armed conflict is not protected, and liability attaches.

Nations are further protected in times of peace from unwarranted and unauthorized intrusions. A state is authorized to take countermeasures under international law when it perceives that its legal rights have been violated by another state and that it must now take an appropriate response. A common example is in the context of a dispute between France and the U.S. over interpretation of a bilateral 1946 Air Service Agreement between the U.S. and

---

[197] Arguably, by these standards, economic embargoes are to be condemned, although unilateral embargoes in which a country simply chooses not to have relations with another may fail short of "interference" or "intervention.

[198] 1928 P.C.I.J. (ser. A) No. 17.

[199] Id

France when France suspended Pan Am flights to Paris. The U.S. perceived that France had interfered with U.S. sovereign affairs and suspended French flights to Los Angeles. The French then sought relief in arbitration and lost.[200] While some actions may not equate to uses of force or acts of aggression, such acts may violate the principles found in various treaties and conventions.

c. *Conventions and Treaties Applicable During Peace and Crisis* – Below is a brief overview of the conventional law that may have a bearing upon information operations during peacetime and crisis.[201] When considering these conventions and treaties, the net effect principle should be used to determine the applicability of the law.

(1) *The United Nations Convention on the Law of the Sea*[202]-- At first glance it may appear that this Convention would have no bearing upon information operations. However, information operations very easily fall within the prejudicial activities prohibited by the Convention. This Convention provides for "innocent passage" in Article 17: "ships of all States, whether coastal or land-locked, enjoy the right of innocent passage through the territorial sea." Article 19 defines passage as "innocent so long as it [the ship's passage] is not prejudicial to the peace, good order or security of the coastal state."[203] The Convention

---

[200] Case Concerning Air Services Agreement Between France and the United States, Arbital Award of December 9, 1978, UNRIAA 417, 443-46.

[201] *See infra* note 237 and accompanying text discussing applicability of treaties and conventions during times of armed conflict and war.

[202] United Nations Convention on the Law of the Sea, opened for signature Dec. 10, 1982, UN Doc. A/CONF.62/122 (1982).

[203] Id.

sets forth activities which are "prejudicial" to the integrity of the coastal state. These prejudicial activities include:

- any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal state, or in any other manner in violation of the principles of international law embodied in the UN Charter;
- any act aimed at collecting information to the prejudice of the defence or security of the coastal state;
- any act of propaganda aimed at affecting the defense or security of the coastal state; and
- any act aimed at interfering with any system of communication or any other facilities or installation of the coastal state.[204]

These prejudicial activities would prohibit a state from conducting information operations while either passing through a nation's territorial waters or while on the high seas. While in the territorial waters, if a ship is claiming innocent passage it may not take any action prejudicial to the coastal state. Therefore, it could not launch an information operation, collect any information which may be prejudicial to the defense or security of the coastal state, aim any propaganda at the coastal state, or interfere with the coastal state's communications system.

While on the high seas, Article 109 prohibits unauthorized broadcasting to shore. Article 109 provides that all "States shall cooperate in the suppression of unauthorized broadcasting from the high seas" and defines unauthorized broadcasting, for the purposes of this Convention, as "the transmission of sound radio or television broadcasts from a ship or installation on the high seas intended for reception by the general public contrary to

international regulations."[205] Thus, a nation could not sit off shore and broadcast propaganda, such as a false news broadcast relaying misinformation set to affect the population of the coastal state.

(2) *The International Telecommunications Convention of 1982 (Nairobi Convention)*[206]-- This convention provides a nation the means to interrupt communications and intercept information operations using the telephone lines if that nation deems the transmission dangerous to the security of that nation.[207] Thus, a nation could disrupt information attacks which come over the telephone lines, which would include all computer-based attacks using the internet or a similar network. Members may "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws, to public order or to decency, provided that they immediately notify the office

---

[204] Id., at art 19.

[205] The internal regulation referenced in Article 109 is the *International Telecommunication Convention,* Malaga-Terremolinos, Oct. 25, 1973, 28 U.S.T. 2495, T.I.A.S. NO. 8572; International Telecommunication Convention, Nairobi, Oct. 1982, see S. EXEC. REP. NO. 4, 99th Cong., 1st Sess. (1986) (hereinafter Nairobi Convention).

[206] Id.

[207] *See* John Davidson Thomas, *International Aspects of the Mobile Satellite Services,* 43 FED. COM. L.J. 45, 46 (1990) ("Life today as we know it would be impossible without satellite communication. Today, more than any other time in history, satellites allow us instant visual access to events clear across the world. We can witness the drama of the Olympics and chart the developments and horror of war from our homes. These are the most visible feats of satellite communication. Yet communications satellites also play an equally dramatic, if unseen, role in our daily lives. Since the 1970s, communications satellites have handled a large percentage of such basic services as telephone traffic and international telex. The large-scale proliferation of personal computers and modems has given birth to digital information services transmitted across phone lines using satellites and other technologies."). *See also* Harold M. White, Jr., & Rita Lauria, *The Impact of New Communication Technologies on International Telecommunication Law and Policy: Cyberspace and the Restructuring of the International Telecommunication Union,* 32 CAL. W. L. REV. 1 (1995).

of origin of the stoppage of any such telegram or any part thereof, except when such notification may appear dangerous to the security of the State."[208] It permits Members to "cut off any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."[209] Members may reserve the right "to suspend the international telecommunication service for an indefinite time, either generally or only for certain relations and or for certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other members through the medium of the Secretary-General.[210] It also provides that all "stations, whatever their purpose, must be established and or practiced in such a manner as not to cause harmful interference to the radio service or communications of other Members or of recognized private operating agencies, or of other duly authorized operating agencies which carry on radio service, and which operate in accordance with the provisions of the Radio regulations."[211]

One could argue that this convention does not prohibit all information operations. For example, Article 38, paragraph 164, provides that military radio installations "must, so far as

---

[208] Nairobi Convention, *supra* note 206, at art. 19, para. 132.

[209] Id., at art. 19, para. 133.

[210] Id., at art. 20, para. 134.

[211] Id., at art. 35, para. 158. The International Telegraph Union (1865) and the Radiotelegraph Union (1906) merged in 1932 and created the International Telecommunications Union (ITU). Now a specialized agency of the United Nations since 1947, it is an autonomous, treaty-based, public international organization which is charged with reconciling conflicting interests in the allocation of international spectrum. The ITU oversees the development and coordination of international communications today.

possible, observe . . . the measures to be taken to prevent harmful interference."[212] "Harmful interference" is defined in Annex 2 to the Convention as "that interference which endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulation."[213] Thus, it appears that the military could use its radio installations to conduct information operations as long as it did not cause harmful interference to radio navigation service or other safety services or a radio communication service. Annex 3 to the Convention contains the Agreement between the United Nations and the International Telecommunication Union. Article XVI of this Agreement provides that the "United Nations undertakes to operate the telecommunication services under its control in accordance with the terms of the International Telecommunications Convention and the regulations annexed thereto."[214] The International Telecommunication Convention may further constrain the information war planner. It states that, "[a]ll stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful

---

[212] Id., at art. 38, para. 164.

[213] Id., at Annex 2. *See* Manfred Lachs, *Views from the Bench: Thoughts on Science, Technology and World Law,* 86 AM. J. INT'L L. 673, 678 (1992) (As a result of the evolution of the law on the allocation of wavelengths and frequencies, the "well-known formula 'harmful interference' has become essential. 'The working of radiotelegraph stations shall be organized, as far as possible, in such manner as not to interfere with the working of other stations of the kind.' Over half a century ago, the Institute of International Law described as 'innocent' a 'simple' passage of wavelengths over territories of other states. Today, thousands of waves cross the territories of states. Telecommunications has grown; the spectrum has expanded five thousand times (the desired spectrum, 500-3000 megahertz, may be used with greater economy). A host of services are in operation, including radio communication, cosmic signals, broadcasting and telephones, creating a worldwide network reaching the remotest corners of the globe. Though earth itself is a fast traveler – nineteen miles per second in its orbit around the sun – telecommunications has opened a new era in travel and in communications.").

interference to the radio service or communications of other Members . . . ."[215] This would apply to information operations conducted by a Member State it such operations amounted to harmful interference.

(3) *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies (The Outer Space Treaty)*[216]—The use of space is a concern to all nations. The Preamble to the treaty the recognizes "common interests of all mankind in the progress of the exploration and use of outer space for peaceful purposes."[217] The Outer Space Treaty states that "State Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons

---

[214] Nairobi Convention, *supra* note 206, at Annex 3, art. XVI.

[215] Id., at art. 35. A TIME magazine article reported that "the Air Force's latest secret weapon" is a converted cargo plane named Commando Solo which purportedly could "jam a country's TV and radio broadcasts and substitute messages – true or false – on any frequency." *See* Waller, *supra* note 21, at 43. Such activity would appear to be a violation of both the Nairobi and Malaga conventions and Art. 37, which reads, "Members agree to take the steps required to prevent the transmission or circulation of false or deceptive distress, urgency, safety, or identification signals . . . ." Nairobi Convention, at Art. 37. Nevertheless, Article 38 of the same treaty states, "Members retain their entire freedom with regard to military radio installations of their army, naval and air forces." Nairobi Convention, at Art. 38.

[216] Treaty on Principles Governing the Activities of States in the Exploitation and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 UST 2410, 610 UNTS 205 [hereinafter Outer Space Treaty]. *See* Pamela L. Meredith, *The Legality of A High-Tech Missile Defense System: The ABM and Outer Space Treaties,* 78 AM. J. INT'L L. 418, 423 (1984) (hereinafter Meredith) ("The Outer Space Treaty is commonly referred to as the 'Constitution of Outer Space.' It sets forth the main principles and guidelines for the activities of states in outer space.").

[217] Id., at pmbl. *See* Meredith, *supra* note 217, at 423 ("The UN Committee on the Peaceful Uses of Outer Space [Legal Sub-committee] has been concerned for many years with 'matters relating to the definition and/or delimitation of outer space and outer space activities. . . .'").

or any other kinds of weapons of mass destruction. . . ."[218] At this time, the term weapons of mass destruction generally refer to nuclear, chemical and biological weapons, and it is unknown whether the destructive potential of information weapons would shift them into this category of weapons. The Outer Space Treaty also states, "[t]he moon and other celestial bodies shall be used by all State Parties to the Treaty exclusively for peaceful purposes. . . [T]he testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden."[219]

As the term "celestial bodies" refers only to natural bodies, such as the moon, asteroids, and planets, not to man-made satellites, it does not appear to limit the scope of information operations, particularly offensive information activities by satellite. However, it can be argued that the language in the preamble limiting the use of outer space to peaceful purposes, would prohibit using something in space as a means of warfare including a satellite as part of an information operation. Under this treaty and other space treaties, states are

---

[218] Id., at article IV. *See* Meredith, *supra* note 217, at 423 ("Article 4 of the Outer Space Treaty deals with the use of outer space for peaceful purposes. Although the request for peaceful use (Art. 4, para. 2) refers specifically to 'the moon and celestial bodies,' it is generally taken as a reference to outer space as a whole. The term 'peaceful' is generally taken to mean nonaggressive as opposed to nonmilitary. Accordingly, military uses of outer space are permitted (insofar as they do not amount to aggression). The first paragraph of Article 4 provides an exception regarding the deployment in earth orbit of nuclear weapons and other weapons of mass destruction. Antiballistic missiles based on laser or particle beam techniques are not weapons of mass destruction. Since they are meant to be a defense system, they are by definition nonaggressive, and their deployment in earth orbit would therefore not represent a violation of international space law."). *See also* Captain Michael G. Gallagher, U.S. Army Reserve, *Legal Aspects of the Strategic Defense Initiative,* 111 MIL. L. REV. 11 (1996).

[219] Id. Similar language is included in the Treaty Governing the Activities in Outer Space, on the Moon, and Other Celestial Bodies, G.A. Res. 34/68, 34 U.S. GAOR Supp. (no. 46) at 77, U.N. Doc. A34/46 (1979) (hereinafter Outer Space Treaty).

responsible for insuring that space is used for the "benefit of mankind" and for "peaceful purposes."[220] The term "peaceful purposes" causes many debates, though the term "peaceful" is generally taken to mean non-aggressive as opposed to nonmilitary activities or purposes.[221] This is an extremely important distinction because of the dual use nature of satellites. An aggressive use of satellites would clearly be in contravention of the convention's "peaceful" intent."[222]

(4) *Convention on International Liability for Damage Caused by Space Objects*[223]-- This Convention holds a launching State absolutely liable under Article II to pay

---

[220] Outer Space Treaty, *supra* note 220. *See generally* Harminderpal Singh Rana, *Note: The "Common Heritage of Mankind" & The Final Frontier: A Revolution of Values Constituting the International Legal Regime for Outer Space Activities,* 26 RUTGERS L. J. 225 (1994).

[221] Meredith, *supra* note 217, at 423, citing S. GOROVE, STUDIES IN SPACE LAW: ITS CHALLENGERS AND PROSPECTS, 85-94 (1977); S. H. LAY & H. TAUBENFELD, THE LAW RELATING TO ACTIVITIES OF MAN IN SPACE 25 (1970); N. MATTE, SPACE POLICIES PROGRAM TODAY AND TOMORROW 68 (1980). *See also* BRUCE A. HURWITZ, THE LEGALITY OF SPACE MILITARIZATION 69 (1986) (hereinafter HURWITZ) (the author concludes that military activities are legal when "peaceful," by which is meant "nonaggressive and beneficial.").

[222] *See* HURWITZ, *supra* note 223, at 128-132 (The author examines antisatellite (ASAT) programs and concludes that "non-nuclear ASAT weaponry is . . . legal." He asserts that ASAT weapons that are not weapons of mass destruction are legal according to the letter of the Outer Space Treaty, but when considering the spirit of the Treaty, "the conclusion appears to be that anti-satellite weapons are legal, de lege lata, but should be illegal, de lege ferenda." Because lasers can be used for beneficial civilian purposes, "an across-the-board prohibition on the use of space-based lasers would not be acceptable," and "[t]he overwhelming opinion is that the intended laser weapon is not a violation of the" Outer Space Treaty.). *See generally* Major John E Parkerson, Jr., *International Legal Implications of the Strategic Defense Initiative,* 116 MIL. L. REV. 67, 81 (1987) ("Senator Albert Gore, representing the United States before the U.N. General Assembly in 1962, emphasized the point that 'the test of any space activities must not be whether it is military or non-military, but whether or not it is consistent with the United Nations Charter and other obligations of law.'").

[223] Convention on International Liability for Damage Caused by Space Objects, March 29, 1972, 24 U.S.T. 2389, T.I.A.S. NO. 7762, 961 U.N.T.S. 187 (assigned responsibility to

compensation for damage caused by its space object on the surface of the earth or to aircraft flight. Damage is defined in Article I to include "loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations." Because this definition does not limit how the space object causes the damage, this damage arguably could include damage caused by information warfare activities that use satellites to cause damage on the surface of the earth or to aircraft in flight.[224] Article VI allows for exoneration of liability if the action taken did not violate international law. Thus, active defensive measures, launched in self-defense to an attack or threat of attack, would be within legal bounds, and liability would be exonerated.

(5) *Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT)*[225] -- The Preamble and Article 1 of the INTELSAT Agreement considers the relevant provisions of the Outer Space Treaty which provide that "that outer space shall be used for the benefit and in the interests of all countries" for peaceful purposes.

---

launching nation for damages caused by its spacecraft) (hereinafter Liability Convention). Like The Outer Space Treaty Preamble, the Preamble to the Liability Convention recognizes "the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes." However, "peaceful purpose" is not defined. Article III of the Convention requires parties to "carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations . . . " and Article IV requires parties not to place "in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction" and requires parties to use the moon and other celestial bodies "exclusively for peaceful purposes."

[224] Id

[225] International Telecommunications Satellite Convention (INTELSAT), Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT), with annex, August 20, 1971, 23 U.S.T. 3813, T.I.A.S. 7532 (hereinafter INTELSAT Convention).

Article III(a) states that "INTELSAT shall have as its prime objective, the provision, on a commercial basis, of the space segment required for international public telecommunications services of high quality and reliability to be available on a nondiscriminatory basis to all areas of the world." Article III(d) states that the "INTELSAT space segment may also, on request and under appropriate terms and conditions, be utilized for the purpose of specialized telecommunications services, either international or domestic, other than for military purposes . . . ." Unfortunately, the phrase, "other than for military purposes" is not defined; however, it has been interpreted to mean "no military use."[226] Thus, this agreement prohibits the military from conducting information operations using INTELSAT stations. Any attempted information operations which causes interruption of the telecommunications services or denial of services would be a violation of the agreement.

(6) *Convention on the International Maritime Satellite Organization (INMARSAT)*[227] -- The INMARSAT Preamble also reflects the Outer Space Treaty's concern for the use of space to the benefit of all humanity[228] and for peaceful purposes.[229] New policy

---

[226] *See* Morgan, *supra* note 6, at 293 ("INTELSAT is proscribed from providing 'specialized telecommunications services' for military purposes." INTELSAT Convention at Art. IIId).

[227] Convention on the International Maritime Satellite Organization (INMARSAT), Sept. 3, 1976, 31 U.S.T. 1, T.I.A.S. 9605 and Operating Agreement on the International Maritime Satellite Organization (INMARSAT), with annex, Sept. 3, 1976, 31 U.S.T. 135, T.I.A.S. 9605 (hereinafter INMARSAT Convention).

[228] Id.

[229] Id.

guidance from the INMARSAT Legal Counsel issued in 1994 attempted to define what is military use of the system relative to "peaceful purpose."[230]

---

[230] INMARSAT Guidelines to all Signatories for Use of INMARSAT by Armed Forces, June 28, 1994 (on file in the Library, The Judge Advocate General's School, U.S. Army, Charlottesville, Virginia); INMARSAT General Counsel Legal Opinion on INMARSAT Use by Armed Forces, November 8, 1994 (on file in the Library, The Judge Advocate General's School, U.S. Army, Charlottesville, Virginia). Telephone interviews with Alan Aukenthaler, General Counsel, INMARSAT, London, England (Feb. 4,5,7 & 9, 1997). Telephone interviews with Dr. Wolf von Noorden, Legal & Regulatory Affairs, Vice-President, Atlas Telecommunications S.A., Brussels, Belgium, (Feb. 7 & 10, 1997) (first INMARSAT General Counsel, 1980-1994). The new guidelines include the following:

> • Use of the INMARSAT system by military forces while not involved in armed conflict or any other threat to or breach of the peace is permitted;
>
> • Use by peacekeeping and peace-making forces acting under the auspices of the United Nations in implementation of UN Security Council decisions is permitted, even if engaged in armed conflict to accomplish their UN mission;
>
> • Use during armed conflict by forces not acting under UN auspices is, in principle, not permitted. There is an exception permitting use to support individual or collective self-defense against armed attack, but this exception would not include preventive action or self-help in the absence of armed attack, or use by government or rebel forces engaged in domestic civil war not involving subversion by a foreign State;
>
> • Use will always be permitted for distress and safety communications and for communications relating to protection of wounded, sick, shipwrecked, prisoners of war, and civilians, even if such communications are made by armed forces while engaged in armed conflict;
>
> • Use for private and non-tactical communications that are not related to or in support of the war effort would be permitted;
>
> • As a condition of commissioning of mobile earth stations, the [INMARSAT] Directorate would require governmental undertakings to ensure compliance with these guidelines.

See Wolf D. von Noorden, *INMARSAT Use By Armed Forces: A Question of Treaty Interpretation*, 23 J. SPACE L. 1, 2 (1995). *See also Morgan, supra* note 6.

(7) *Convention on International Civil Aviation (Chicago Convention)*[231] -- As a result of the Soviet Union's shoot down of a Korean Passenger Airline, KAL 003, in 1983, the delegates to the International Civil Aviation Organization adopted article *3 bis*, which provides that "every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of persons on board and the safety of aircraft must not be endangered."[232] This will have an impact on information operations which could potentially interrupt air traffic control, interfere with radio transmissions, or confuse navigational aids which cause the crash of aircraft. Such operations would focus on disrupting radar sites, global positioning systems (GPS), and air traffic control systems. However, information operations which would disrupt telecommunications systems or electrical systems may also affect air traffic control systems through an interlink of the systems. Although an information operation may be targeted at a military target, by the interconnectedness of the information infrastructure, the operation may interfere with civil

---

[231] Chicago Convention, *supra* note 117. Although Article 3 bis is not in force for the United States, the Legal Counsel for the Department of Justice opined in a formal memorandum of law dated July 14, 1994, that article 3 bis is declaratory of customary international law. "Article 3 bis should be understood to preclude states from shooting down civil aircraft suspected of drug trafficking, and the only recognized exception to this rule is self-defense from attack. We understand that the United States has not yet ratified Article 3 bis. There is, however, support for the view that the principle it announced is declaratory of customary international law." Dep't of Justice, Memorandum for Jamie S. Gorelick Deputy Attorney General from Walter Dellinger, Assistant Attorney General, Subject: United States Assistance to Counties That Shoot Down Civil Aircraft Involved in Drug Trafficking, July 14, 1994, at 3 (footnotes omitted).

[232] Id.

aircraft. Such potential interference with civil aircraft must be weighed against the military necessity of the target.[233]

2. *Periods of Armed Conflict and War* -- Conventional and customary international law regarding armed conflict and war is referred to as the Law of War or the Laws of Armed Conflict (LOAC).[234] This body of international law, which developed over the centuries as states attempted to control warfare, especially as technology increased the lethality of weapons,[235] is much clearer than the body of law applicable during peacetime and crisis on

---

[233] *See infra* note 257 and accompanying text.

[234] International armed conflict is defined in Common Article 2 to the four Geneva Conventions, one of the four being the Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T 3114, 75 U.N.T.S. 31; and further defined in, for those states a party to the two Additional Protocols to the Geneva Conventions, Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, art 1. para. 3.-4., U.N. Doc. A/32/144. Annex I (1977), 16 I.L.M. 1391 (1977); and Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, art 1., U.N. Doc. A/32/144. Annex II (1977), 16 I.L.M. 1442 (1977).

[235] Lieutenant General Xing Shizhong, President of National Defense University, People's Liberation Army, China, Address at the United States National Defense University, Oct. 1996 ("History has shown that progress in science and technology has always led to a leap in the social productive forces, greatly increasing the social production, and speeding up the progress of social development. The same is true in the military field. The revolutionary development in science and technology has always been the motive force for the revolutions in the military field. In ancient times, wars were fought bare-handed. The emergence of smeltery technology made possible fighting with cold weapons. The invention of gunpowder and explosives brought about hot weapons to the battlefield. More recent technological developments gave birth to inter-combustion engines and other mechanical systems, thus revealing mechanized warfare. By 1950's, long range nuclear weapons were manufactured due to the development in nuclear and rocket technologies. Today, all signs suggest the huge destructive power of long range nuclear weapons and the swift development of information and computer technology may bring forth a new form of warfare to the human world, that is, the information warfare under nuclear deterrence conditions. As information and knowledge are uniquely characterized by their global extension, light speed transmission, non-liner

the issues of use of force and intrusions into the sovereign territory of another state. As there is much more written on LOAC, this section will provide only a brief overview of the aspects of conventional and customary law applicable to information operations.

a. *Conventions and Treaties Applicable During Armed Conflict and War* – Some conventions and treaties clearly apply during periods of armed conflict and war, such as those discussed below, however, this is not true with respect to all conventions and treaties. Some treaties may terminate or be suspended due to breach or impossibility of performance of fundamental change of circumstances due to armed conflict or war, however, "no international tribunal has had occasion to decide a case involving the question of the effect of war upon treaties . . . ."[236] Nevertheless, some multilateral conventions provide for their effect in time of war, such as the Chicago Convention.[237]

---

effect, inexhaustibility and wide obtainability, they have become important amplifiers of the anti-personnel and even destructive forces in modern warfare. One has good reason to believe that the mode of warfighting will hence experience revolutionary changes in 20 to 50 years. For instance, information warfare may become the focus in future wars, and the control information and its systems will gradually become the central issue at the operational level of war. In future, information will be one of the most important war resources, and a field commander will have to win victory by first stressing flexible employment of information systems as with his air and naval forces . . . . The development of information technology will further blur the difference between the front and rear, the battlefields will be more fluent in nonlinear and frontless shape. The operations on the sea, on the ground, in the air and in the space will be more closely linked together, forming a true multi-dimensional battlefield. This unprecedented change in the perception of both time and space will not only provide the advantageous conditions for, but also great challenges to the field commander to visualize the whole situation and to organize command and control.").

[236] DA PAM 27-161-1, *supra* note , at paras. 8-32, 8-33, & 8-34. Concerning multilateral conventions the following points should be considered in conducting the analysis: (a) Vis-à-vis parties to the conflict: absent a specific termination or suspension clause, the obligations of a treaty may continue to exist between treaty parties that are not a party to an armed conflict depending upon the intrinsic character of the treaty; (b) Vis-à-vis non-parties to the conflict: belligerent state has the duty under the law of war to respect the rights of neutral states and vice versa. Moreover, contractual obligations imposed by convention may be

While the Law of Armed Conflict is also referred to as the Law of War, the terms armed conflict and war have different meanings. The term "armed conflict" is found in common Article 2 of the Geneva Conventions.[238] Commentaries on the Geneva Conventions indicate that this term was specifically chosen over the term "war"[239] because of its broader scope in not being tied to the specific legal concepts tied to the term war.[240] As Article 2 concerns armed conflict of an international nature – between two sovereign states – this is commonly referred to as the law of international armed conflict. "Any difference arising

---

modified by specific terms of the convention, general principles of treaty termination or suspension, and operation of Article 103 of the UN Charter.

[237] Chicago Convention, *supra* note 117, at Article 89, specifies that "[i]n the case of war, the provisions of this Convention shall not affect the freedom of action of any of the contracting States affected, whether as belligerents or neutrals. . . ."

[238] Id.

[239] Bruce V. Bigelow, *Cyberwarriors Pentagon's New Priority: Train Troops to Cripple Computers - and Enemy Forces They Control,* THE SAN DIEGO UNION-TRIBUNE, August 13, 1995, at A-1 (When considering the application of the LOAC to information warfare, one has to consider what is an act of war, in fact, in contemporary society, what is war? War is a legal relationship, initiated by a declaration of war or by an "act of war," for example, an act demonstrating an intention to be at war, or constituting such a serious breach of the rights of another nation that it would be justified in declaring war. The United States was at war with Japan after Pearl Harbor, but it was at war with Germany only after a declaration of war was enacted by Congress. As a result of the United Nations Charter and its mission to quell impending conflict, the concept of war in its legal sense has fallen into disuse. The legal and practical consequences of a state of war are complicated, and are better suited to a state of general war pursuing unconditional surrender than to limited conflicts with limited ends. As a legal matter, termination of a state of war requires a peace treaty, which may be hard to negotiate and conclude. Today's emphasis is on settlement of disputes before they degenerate into war. An "act of War" traditionally has been limited to an "armed attack." What would constitute an act of war in cyberspace? Noting that the Prussian military theorist, Karl von Clausewitz, wrote that the fundamental characteristic of war is violence, Dr. John Alger, Dean, School of Information Warfare, National Defense University, said: "You have to ask now if it [warfare] is still [always] violent. We can control information. We can destroy information. It happens every day [without violence].").

between two states and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the parties denies the existence of a state of war."[241] Conflicts of an internal nature are defined in common Article 3 of the Geneva Conventions. Although LOAC does not specifically apply to internal armed conflict, the United States applies it as a matter of law and policy.[242]

This is specifically why determining the identity of an actor is so crucial. Potentially, actions by both a state actor and a non-state actor could fall under the scope of LOAC. The identity of an actor will also determine whether law enforcement or DoD responds to the intrusion. It is one thing for the military to respond to an intrusion against another state but for the government to unleash the latest information warfare technology on a few bored teenagers or a domestic rebellious faction would be devastating.[243]

---

[240] JEAN PICTET, THE GENEVA CONVENTIONS OF 12 AUGUST 1949, COMMENTARY 29 (1952).

[241] JEAN PICTET, THE GENEVA CONVENTIONS OF 12 AUGUST 1949, COMMENTARY 20 (1958). Unfortunately, today we are unable to forecast reliably what kinds of electronic attack will be considered by a target country or by the world community to be equivalent to an armed attack. The threshold for an action to be considered an "act of war" is so high that the target nation's rights under intentional law will be violated long before reaching the level or an act of war; the sanctions potentially resulting from such violations will be significant long before a state of war is provoked.

[242] *See generally* DEP'T OF DEFENSE, DIR. 5100.77, DOD LAW OF WAR PROGRAM, 10 July 1979. Paragraph E.1.a provides that "[t]he Armed Forces of the United States shall comply with the law of war in the conduct of military operations and related activities in armed conflict, however such conflicts are characterized."

[243] *See* Edward Tenner, *Age of Anarchy in Cyberspace: How Can You Distinguish a Hired Attacker from a Bored Suburban Kid?*, S. CHINA MORNING POST, Feb. 19, 1997, at 13.

The Hague IV Convention and the regulations attached to it represent for the first time the environment of the law of war was codified into treaty law.[244] It also codified the customary law concept that methods of warfare are not unlimited.[245] It also prohibited the destruction or damage of property in the absence of military necessity.

Only the principal provisions of The Hague and Geneva Conventions that directly relate to offensive information warfare are discussed below:

(1) *Regulations Respecting the Law and Customs of War on Land, annexed to Hague Convention No. IV Respecting the Laws and Customs of War on Land*[246] – The Hague Convention establishes that "[t]he right of belligerents to adopt means of injuring the enemy is not unlimited."[247] While the current electronic technological advances did not exist at the time of the drafting of the Hague Convention, many of the non-electronic aspects of information warfare did exist. As such, there are many provisions within the convention, which are applicable to information operations. [248] Article 22 of the annexed Regulations to

---

[244] DEP'T OF ARMY, THE JUDGE ADVOCATE GENERAL'S SCHOOL, OPERATIONAL LAW HANDBOOK, JA 422 5-4 (1996).

[245] Id.

[246] Regulations Respecting the Law and Customs of War on Land, annexed to Hague Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, 205 Consol. T.S. 277.

[247] Id., at art. 22

[248] The following is a list of Hague Convention sections addressing aspect of information operations:

1. Article 23 - "In addition to the prohibitions provided by special Conventions, it is especially forbidden . . . to employ arms, projectiles, or material calculated to cause

the 1907 Hague Regulation Number IV[249] provides the most fundamental customary principle of armed conflict. Article 22 provides that the "right of belligerents to adopt means of injuring the enemy is not unlimited." The principle of limited means has two corollaries: proportionality and discrimination. Proportionality is a very fact-specific concept that limits the use of force, and in practice, proportionality is the balancing between the principles of military necessity and unnecessary suffering. The second principle is discrimination, which restricts methods, weapons, and targets.

---

unnecessary suffering; . . . to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war." Article 27 - "in sieges and bombardments all necessary steps must be taken to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes."

2. Article 24 - "Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible." Article 53 - "An army of occupation can only take possession of cash, funds, and realizable securities which are strictly the property of the State . . . and generally, all movable property belonging to the State which may be used for military operations."

3. Article 3 (of the Convention Proper): "A belligerent party which violates the provisions of the said Regulations shall, if the case demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces."

4. Article 53 - "All appliances, whether on land, at sea, or in the air, adapted for the transmission of news, or for the transport of persons or things, . . . may be seized, even if they belong to private individuals, but must be restored and compensation fixed when peace is made."

5. Article 56 - "The property of municipalities, that of institutions dedicated to religion, charity and education, the arts and sciences, even when State property, shall be treated as private property. All seizure of, destruction or willful damage done to institutions of this character, historical monuments, works of art and science, is forbidden, and should be made the subject of legal proceedings."

(2) Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land[250] -- The Convention on Neutrals prohibits belligerents from erecting "on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea" and from using "any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages."[251] Of possible concern is that article 8 states that a "neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals," however, the "measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Article 8 must be impartially applied by it to both belligerents."[252]

(3) *The Geneva Conventions* -- There are several sections in The 1949 Geneva Convention Number IV Relative to the Protection of Civilian Persons in Time of War which have bearing on information warfare operations. These sections focus primarily upon whether the action resulted in excessive damage not justified by military necessity.[253]

---

[249] Hague Convention No. IV of October 18, 1907, Respecting the Laws and Customs of War on Land, 36 Stat. 2277, T.S. No. 539.

[250] Hague Convention No. V of October 18, 1907, Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 36 Stat. 2310, T.S. No. 540.

[251] Id., at art. 3.

[252] Id., at art. 9.

[253] The applicable provides of the Geneva Conventions include the following:

With respect to information warfare, these sections require that information warfare operations adhere to the strict concept of military necessity and the assessment of potential damage to civilians.

b. *Customary International Law*[254] -- As discussed above with reference to Article 22 of the Hague Convention, the principles of proportionality and discrimination are critical in any discussion and analysis of information warfare during armed conflict and war. operations and warfare. These principles of proportionality and discrimination can be further broken down into three interrelated customary principles of international law: military necessity, unnecessary suffering, and chivalry.[255] There is a continuous balancing of the military commander's mission with the effects of the mission. The common factor among all of these principles is that they look to the net effect of the activity.

(1) *Military necessity* - Focused upon the net effect of the action, military necessity is defined as military operations: undertaken with only that degree and kind of

---

1. Article 53: "any destruction by the Occupying Power of real or personal property belonging individually or collectively to private persons, or to the State, or to other public authorities, or to social or cooperative organizations, is prohibited, except where such destruction is rendered absolutely necessary by military operations."

2. Article 147 - "Grave breaches . . . shall be those involving . . . extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly."

3. Article 148 - "No High Contracting Party shall be allowed to absolve itself or any other High Contracting Party of any liability incurred by itself or by another High contracting Party in respect of breaches referred to in the preceding Article."

[254] *See supra* note 108, and accompanying text.

[255] L. C. GREEN, ESSAYS ON THE MODERN LAW OF WAR 84 (1985).

force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy; with a minimum expenditure of time and life; and, with the application of physical resources.[256] The proportionality element of military necessity does not require a state to limit its means and methods of warfare to a level equivalent to its enemy's weapon systems and force levels. Military commanders may target only combatants and military objectives. Military objectives "are objects which, by their nature, location, purpose, or use, effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack."[257]

(2) Unnecessary suffering and destruction -- also known as the principle of humanity -- states that "[t]he employment of any kind or degree of force not required for the purpose of the partial or complete submission of the enemy with a minimum expenditure of

---

[256] DEP'T OF THE AIR FORCE MANUAL, AFP 110-31, INTERNATIONAL LAW – THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS 1-6 (1976). Reference to military necessity may be found in the Hague Regulations, Art. 23(g), which prohibit the destruction or seizure of the enemy's property, unless a military commander deems it imperatively necessary to the military objective. Allowance for military necessity are also made in the Geneva Conventions, the Cultural Property Convention of 1954, and in Protocol I. *See* DETTER DE LUPIS, THE LAW OF WAR, 334-6 (1987); and H. McCoubrey, *the Nature of the Modern Doctrine of Military Necessity,* MILITARY LAW AND LAW OF WAR REVIEW 229-37 (1991).

[257] Art. 52, para. 2, Protocol I Additional to the Geneva Convention of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Dec. 12,1977, 1125 U.N.T.S. 3, 16 I.L.M. 1391 (the United States has not ratified Protocol I) [hereinafter Protocol I].

time, life, and physical resources, is prohibited."[258] This aspect of customary law also focuses upon the ultimate net effect of the mission. It causes the commander to balance military necessity with the potential suffering and destruction which may occur as a result of the operation.[259]

(3) Chivalry -- This principle forbids dishonorable (treacherous) means, dishonorable expedients, and dishonorable conduct during armed conflict.[260] The principle of chivalrous conduct is implemented through provisions that concern perfidy and ruses of war.

(a) Perfidy – Acts inviting the confidence of an adversary to lead him to believe that he or she is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy.[261] Perfidy consists of committing a hostile act under the cover of a legal protection such as pretending to surrender.[262]

---

[258] DEP'T OF THE AIR FORCE, THE AIR FORCE JUDGE ADVOCATE GENERAL'S SCHOOL, THE MILITARY COMMANDER AND THE LAW 581 (Sept. 1994).

[259] ROGERS, *supra* note 106, at 7.

[260] MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 34 (2d ed. 1992).

[261] Protocol I, *supra note 257*, at arts 37-39.

[262] FREDERIC DE MULINEN, HANDBOOK ON THE LAW OF WAR FOR ARMED FORCES 83, 97 (1987).

(b) Ruses – Ruses of war or stratagems are any acts of deception not amounting to perfidy but which are intended to mislead the enemy or induce him or her to act recklessly. Examples of ruses include: mock operations, decoys, misinformation, and technical means of deception.[263] These are not violations of LOAC, however, information operations must be carefully scrutinized to ensure that they do not amount to perfidy.

(4) *Incidental injury and collateral damage* - an important distinction between peace and crisis operations and operations during armed conflict and war is that for lawful combatants, it is not unlawful to cause incidental injury or death to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military objective.[264]

The application of the principles of proportionality and discrimination to information operations is essential in all information operations, not just those during armed conflict. In both offensive and defensive operations, the net effect of the operation must be determined with clarity. The target must be identified, the technique chosen and then a balancing test imposed between the requirements of the military mission and the possible resultant damage.

---

[263] Id.

[264] ANNOTATED SUPP., *supra* note 107, at para. 8.1.2.1 ("It is not unlawful to cause incidental injury or death to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military objective. Incidental injury or collateral damage should not, however, be excessive in light of the military advantage anticipated by the attack. Naval commanders must take all practical precautions, taking into account military and humanitarian considerations, to keep civilian casualties and damage to the absolute minimum consistent with mission accomplishment and the security of the force. In each instance, the commander must determine whether incidental injuries and collateral damage would be excessive, on the basis of an honest and reasonable estimate of the facts available to him, including the need to conserve resources and complete the mission successfully, whether to adopt an alternative method of attack, if reasonably available, to reduce civilian casualties

IV. The Framework for Analysis of Information Operations

A. The Framework of Analysis

The previous section discussed the current state of international law and how such law may be applied to information operations. This section provides a framework for analysis of an information operation. While some aspects of an information operation may not fit perfectly under the law, there is sufficient ambiguity in the law to expand and cover the information operation. The framework is found at Appendix A.

B. Application of Framework of Analysis to Sample Scenarios

The application of the framework to the following scenarios demonstrates that the current legal framework is applicable to information operations and that a new legal paradigm is not necessary at this time.

1. *Scenario Alpha* -- During the past several years, a disruptive group known as "The Rolling Pebbles," claimed responsibility for a campaign of attacks against State A. These attacks included both the use of conventional bombs and information warfare methods. The Rolling Pebbles recently destroyed State A's electric power grid station and telephone facilities with conventional bombs. They also hacked into State A's railroad computer system and inserted a malicious computer virus into it which caused trains to be misrouted

---

and damage." (footnotes omitted)).

and crash. The Rolling Pebbles targeted these facilities in protest over State A's research on pet rocks. The Rolling Pebbles launched the attacks from various places. State A's military is tired of this activities of The Rolling Pebbles and is proposing to use its military information warriors to launch a computer-based network attack at The Rolling Pebbles through the Internet.

a. Analysis of Scenario Alpha Using the Analysis Framework

A. Peacetime usage of Information Operations – Yes.
1. What occurred? The Rolling Pebbles attacked State A's power and telephone facilities and hacked into its railroad system causing great havoc. State A's armed forces want to use military information warriors to launch an attack on The Rolling Pebbles through the Internet.
2. Determine identity of actor. The Rolling Pebbles – non-state actor so discontinue analysis; State A is a state actor.
3. What was actor's intent behind the information operation? The Rolling Pebbles were carrying out terrorist criminal activities against State A to force it to change its activities regarding pet rocks. State A believes they need to take the information operation in order to defend their country from The Rolling Pebbles.
4. What was result of actor's information operation? State A believes that it will destroy The Rolling Pebbles morale and they will cease their operations against State A. The Rolling Pebbles' criminal activity caused much harm to State A.

b. *Discussion of Scenario Alpha Based on the Analysis Framework* --

Although State A is correct in saying that its armed forces must defend State A, however, this is a matter for State A's law enforcement agencies because The Rolling Pebbles are non-state actors who have committed criminal acts against State A. Thus, State A's armed forces would be wrong in launching an Internet attack against these non-state criminal actors based on the facts provided. The armed forces should refer the matter to the appropriate law enforcement agency.

2. *Scenario Bravo* -- Tensions between State A and its neighbor State B increase after negotiations break off over a disputed area of land. A clever State A military information warrior reports that he has gained access to the computer that serves as the host for State B's military command and control (C2) network. He proposes implanting a "logic bomb" into the system. The logic bomb will remain inert and harmless for the present, but State A could activate it in the event of any future armed conflict to degrade State B's command and control (C2) network. This C2 network also controls the Global Positioning System (GPS). In State B, the GPS is a dual use system which both the military and the civilian sectors share. State A wants to ensure that State B never knows who was responsible for destroying their C2 network and plans to conduct the insertion using covert means.

a. *Analysis of Scenario Bravo Using the Analysis Framework*

A. Peacetime usage of Information Operations – Yes.
1. What occurred? Nothing yet, although State A is contemplating inserting a logic bomb into State B's C2 network to destroy it in the event of armed conflict between the two states. State A will undertake this insertion as a covert activity.
2. Determine identity of actor. State A- a state actor but its identity will remain unknown to State B.
3. What was actor's intent behind the information operation? State A will argue that its action is anticipatory self-defense to some future conflict between State A and State B.
4. What was result of actor's information operation? State A's insertion of the logic bomb and its activation may bring about separate results. The insertion of the logic bomb is an interference with State B's sovereignty whether or not the logic bomb is activated. The mere presence of the logic bomb creates a vulnerability in State B's C2 system. If State B finds out about it and knows State A is responsible, it may seek to take an action in response to State A's insertion activity. Also, once State A activates the logic bomb, it will affect not only the military C2 network, but also both military and civil aircraft. This will occur because the GPS system, which is linked with the C2 system, will fail once the C2 system is destroyed.
5. Does the activity violate any existing international conventions? Yes.
    a. As the State A information warriors would hack into State B's C2 network through telephone lines, this would violate The International Telecommunications Convention of 1982 (Nairobi Convention): Art 35, para 158 - Ground stations must not cause harmful interference, and Art

38, para 164 - Military radio installations must prevent harmful interference as far as possible.

b. Once the logic bomb destroys the C2 network, it will also destroy the GPS systems and affect both military and civil aircraft that rely on the GPS system for direction. Thus, this action will violate the International Civil Aviation (Chicago Convention): Art. *3 bis* – "every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of persons on board and the safety of aircraft must not be endangered."

6. Does the activity violate any domestic laws or agreements? It may violate several laws unless State A takes into consideration the following laws when planning the covert activity:

a. Executive Order 12333 – United States Intelligence Activities
b. Covert Actions – 50 USC 413b(e)
c. Traditional Military Activities – 50 USC 413e

7. Does the activity cross the proscriptive threshold of use of force of article 2(4) of the UN Charter? Whether State A's insertion of the logic bomb amounts to a use of force under article 2(4) is unclear. State A will argue that mere insertion of the logic bomb is not a use of force, and under the net effect principle, there has been no damage to State B by the mere insertion of the logic bomb. Additionally, the insertion does not cause any damage to State B. State A's activation of the logic bomb may cross the threshold of article 2(4) if State A activates the device even though State B never intended nor gave any indications it would launch an attack on State A. If, however, an attack by State B was imminent or occurred and State activates the logic bomb, State A would claim self-defense.

7.a. If it was authorized by the Chapter VII authority of the UN Security Council, then the fundamental principles that reflect customary international law apply to information operations that amount to the use of force under Article 41 of the UN Charter during UN operations in which member states are not parties to an international armed conflict. If member states are parties to an international armed conflict, then law of armed conflict applies. Not applicable here until the logic bomb breaks out. Then if it affects something like the GPS, then it will need to be analyzed in terms of proportionality and discrimination.

7.b. If it was not authorized by Chapter VII authority of UN Security Council, then use of force may nevertheless still be authorized under the inherent right of individual or collective self-defense as recognized by Article 51 of the UN Charter. Regardless of whether the use of force is legitimate self-defense, the law of armed conflict applies. In order to claim self-defense for both the insertion and the activation, State A would have to demonstrate an imminent or actual attack by State B.

B. Armed Conflict and Wartime usage of Information Warfare. No. This would apply only if State A were facing an imminent or actual use of force by State B and State acted in self-defense. Based on the facts, this is not the case until the logic bomb breaks out. Then if it affects something like the GPS, then it will need to be analyzed in terms of proportionality and discrimination..

b. *Discussion of Scenario Bravo Based on the Analysis Framework* -- Under the framework provided, although tensions are high, it is still a peacetime environment. What has occurred so far is that State A has gained access to State B's C2 server host. At this time, there is a proposal to insert a "logic bomb." The actor here is State A, a state actor, and it is considering this action as an act of self-defense should State A and State B move into toward armed conflict sometime in the future. Despite the assertion that the integrity of an important national asset has been violated, and a significant vulnerability has been created, it does not appear that any damage would result from insertion of the logic bomb. A case can be made that merely accessing State B's C2 network is an interference in the internal affairs of State B because the intent of the insertion and the result of any activation would be to disrupt State B's C2 network. On the other hand, an argument can be made that such action is no different than having prepositioned someone inside State B who can carry out a mission of destroying the C2 network upon command. The net effect, the intent and the result of the information and non-information operation, is the same. Whether this interference amounts to a use of force is not clear, however, it is unlikely.

The activation of the logic bomb, however, raises other issues. State A will argue the activation is an act of self-defense in response to a hostile act by State B. The problem here is that destroying the C2 network also interferes with the dual use (military/civilian) GPS system. State A must carefully consider activating this logic bomb in light of this result. If this occurs during peacetime or crisis, then there may be violation of article *3bis* of the Chicago Convention, which prohibits the use of any weapon against civil aircraft in flight and endangering both the safety of the passengers and the aircraft. By shutting down the C2

network, and consequently shutting down the GPS, this endangers the safety of persons on civil aircraft. It would be no different from State A shooting the aircraft down from the sky. Unless State A can demonstrate it took this action in self-defense, it will probably be liable under the Chicago Convention for the damages caused by the logic bomb. If State A wants to activate the logic bomb during armed conflict or war, the C2 network is a legitimate military target, even if there is a dual use aspect to such a network. State A must weigh the proportionality of its action by balancing the military necessity of destroying the C2 network and the unnecessary suffering which will be cause by planes crashing. If destroying State B's C2 network is a critical military necessity, then State A should try to activate the logic bomb at a time when there were none, or only a few aircraft in the sky and diminish the expected incidental injury and collateral damage. State A would not be liable for the deaths of civilians if its actions were consistent with the Regulations Respecting the Laws and Customs of War on Land, annexed to Hague Convention No. IV, The 1949 Geneva Convention No. IV Relative to the Protection of Civilian Persons in Time of War, the Annexed Regulations to the 1907 Hague Regulation No. IV, and customary law principles.

3. *Scenario Charlie* -- Tensions continue to escalate between State A and State B. One of State A's finest military information warriors proudly announces that he has found a way to gain access to State B's national radio and television networks and to override its broadcasts with State B's "programs." He proposes broadcasting a program made by "morphing" technology that makes State A's false broadcasts indistinguishable from the State B's overtaken network's usual broadcasts. State A wants to depict State B's "Undemocratic Democratic" Leader, General Stone, in an unfavorable manner to State B's

populace. State A developed a morphed broadcast which shows General Stone talking with a few of his cronies about the incredible profits he is making from clandestine deals in supplying stones to State A's pet rock supplier. He also tells his group of obsequious supporters that he is using The Rolling Pebbles as a pawn in State B's struggle with State A over the disputed territory. State A clearly expects that such a broadcast would erode domestic public support for State B's leadership and drive a wedge in any existing cooperative arrangement between State B and The Rolling Pebbles.

a. *Analysis of Scenario Charlie Using the Analysis Framework* --

A. Peacetime/crisis usage of Information Operations. Yes
1. What occurred? Nothing has happened yet, but State A proposes to broadcast a false "morphed" program into State B.
2. Determine identity of actor. State A, state actor.
3. What was actor's intent behind the information operation? State A wants to interfere in State B's internal affairs and disrupt the pubic confidence in State B.
4. What was result of actor's information operation? Although it has not happened yet, State A expects that the broadcast will affect the entire populace of State B and undermine its confidence in General Stone.
5. Does the activity violate any existing international conventions? Yes.
    a. If State A broadcasts this morphed program from a ship on either the high seas or in State B's territorial seas, it will violate the United Nations Convention on the Law of the Sea: Art. 17 – Ships of all states enjoy innocent passage through the territorial sea but under Art 19, such passage is not innocent if it involves any act of propaganda aimed at affecting the defense or security of the coastal state, State B. Furthermore, Article 109 provides for the suppression of any unauthorized broadcasting to include "transmission of sound radio or television broadcasts from a ship or installation on the high seas intended for reception by the general public."
    b. Broadcasting the false program would cause harmful interference with the radio services or communications of State B in violation of The International Telecommunications Convention of 1982 (Nairobi Convention): Art 35, para 158 - Ground stations must not cause harmful interference; and Art 38, para 164 - Military radio installations must prevent harmful interference. Annex 2 to the Convention defines harmful interference as that interference "which endangers the functioning of a radio navigation service or of other safety services or seriously degrades; obstructs or repeatedly interrupts a radio commination service." Art 38, para 164, provides that military radio installations "must, so far as

possible, observe . . . the measures to be taken to prevent harmful interference."

c. If State A uses its satellites to broadcast this morphed program clearly aimed to cause unrest in State B, this would probably violate the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space , including the Moon and other Celestial Bodies (Outer Space Treaty): Preamble – the use of outer space for peaceful purposes; and Art III - carry on activities in space in accordance with international law, including UN Charter, which prohibits interference in the internal affairs of other nations.

d. If State A used the INTELSAT stations to broadcast the program, it would violate the Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT) (commercial ground stations): Preamble – refers to Article I of the Outer Space Treaty which states that "outer space shall be used for the benefit and in the interests of all countries," and this broadcast clearly would not be in the interests of all countries; Art III(a) - "INTELSAT's prime objective is the provision, on a commercial basis, of the space segment required for international public telecommunication services of high quality and reliability to be available on a non-discriminatory basis to all areas of the world." Broadcasting of propaganda would be in clear contravention of this article; Art III(d) – "INTELSAT space segment may also, on request and under appropriate terms and conditions, be utilized for the purpose of specialized telecommunications services, either international or domestic, other than for military purposes . . . ." Clearly, if the military uses the INTELSAT to broadcast the morphed program, it will violate this section.

e. Because military use of INMARSAT is not prohibited, State A's armed forces may try to use the INMARSAT system. However, even with the allowance for expanded military uses for peaceful purpose, broadcasting the propaganda would violate the Convention on the International Maritime Satellite Organization (INMARSAT) (maritime mobile stations)Preamble – refers to Article I of the Outer Space Treaty which states that "outer space shall be used for the benefit and in the interests of all countries;" and Art III – provides that the "organization shall act exclusively for peaceful purposes."

6. Does the activity violate any domestic laws or agreements? It may unless State A considers and complies with the following laws:

a. Executive Order 12333 – United States Intelligence Activities: provides that the NCA must approve all peacetime psychological operations.
b. Covert Actions – 50 USC 413b(e)
c. Traditional Military Activities – 50 USC 413e
d. Telecommunications Contracts with commercial companies which may prohibit any such broadcasts.

7. Does the activity cross the proscriptive threshold of use of force of

article 2(4) of the UN Charter? While the broadcast clearly amounts to an intervention in the internal affairs of another country, it does not appear to rise to the level of a use of force under article 2(4).

7.a. If it was authorized by the Chapter VII authority of the UN Security Council, then the fundamental principles that reflect customary international law apply to information operations that amount to the use of force under Article 41 of the UN Charter during UN operations in which member states are not parties to an international armed conflict. If member states are parties to an international armed conflict, then law of armed conflict applies. Not applicable.

7.b. If it was not authorized by Chapter VII authority of UN Security Council, the use of force may nevertheless still be authorized under the inherent right of individual or collective self-defense as recognized by Article 51 of the UN Charter. Regardless of whether the use of force is legitimate self-defense, the law of armed conflict applies. Not applicable here.

B. Armed Conflict and Wartime Usage of Information Warfare - No. Analysis stops here.

b. *Discussion of Scenario Charlie Based on the Analysis Framework* -- This is a period of crisis between State A and State B. State A is the state actor and plans on broadcasting a "morphed" or false propaganda broadcast in State B. These morphing techniques, using computers, generate a realistic video recording indistinguishable from an actual recording. These techniques were used in making the 1994 motion picture FORREST GUMP. The movie character appears to be part of actual thirty-year-old news stories. State A would then transmit this broadcast electronically to State B's network. Clearly, State A's intent in using the morphed video material is to interfere in the internal affairs of State B resulting in an erosion of State B's confidence in its leader. There is considerable international support for the proposition for the duty of states not to intervene in domestic matters of other states in the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N. Doc. A/8028 (1970). Additionally, State A would be broadcasting false propaganda.

This broadcast would violate several international conventions. If such broadcast were sent from a ship in the high seas, it would violate article 109 of The Law of the Sea Convention. If broadcast from an aircraft like Commando Solo, these morphed broadcasts may violate Article 35 of the International Telecommunications Convention (Nairobi Convention), because the false broadcast would "cause harmful interference to the radio service of communications" of State B. However, Article 38 of the Nairobi Convention allows members to retain their entire freedom with regard to the use of military radio installations. Military radio installations must observe measures to prevent harmful interference. Harmful interference is defined as the functioning of a radio navigation service or of other safety services which seriously degrades, obstructs or repeatedly interrupts a radio communication service." This morphed broadcast does not appear to affect the functions of an radio navigation service or safety services. Thus, it appear that Article 38 may allow the military to broadcast from the military aircraft like Commando Solo. State A's armed forces would not be permitted to use the INTELSAT ground stations to broadcast such propaganda because INTELSAT stations may not be used for military purposes. Such broadcast would be prohibited in accordance with the INMARSAT convention and legal guidelines because there is no intended "peaceful purpose."

On the domestic front, State A's armed forces must ensure that they have complied with any domestic laws concerning propaganda. They should consult any Executive Orders such as Executive Order 12333 – United States Intelligence Activities, which provides that the National Command Authority must approve all peacetime psychological operations. In addition, if this action is taken as a covert action it must comply with domestic laws concerning covert activities such as 50 U.S.C. 413b. Additionally, State A may not use any

commercial telecommunications systems to transmit such a broadcast if the contract expressly forbids such transmissions.

It appears that the only way that State A could broadcast this morphed program is with proper domestic government clearances, and in reliance on Art 38, para 164 of the Nairobi Convention.

4. Scenario Delta -- The crisis between State A and State B has reached the point that State A actually believes that State B's air force will mount an air attack against State A within a few days. State A's armed forces propose two methods to counter State B's imminent attack: 1. a preemptive night raid to blow up State B's air control radar for the boarder sector, and 2. use an information operation to put the same facility out of action by electronic means.

a. *Analysis of Scenario Delta Using the Analysis Framework* --

A. Is it peacetime/crisis or armed conflict/war environment? Peacetime/crisis, unless State A affirmatively establishes that State B was going to launch an imminent attack which would make it an armed conflict/war environment and analysis would begin at No. 12 Below.
1. What occurred? State A wants to destroy State B's radar control site with either conventional means or information operations.
2. What is the identity of the actor? State A is state actor.
3. What was actor's intent behind the operation? State A's intent behind their action to destroy the radar control site in anticipatory self-defense which permits State A to strike first when it has a persuasive reason to believe that it is about to be attacked.
4. What was result of actor's information operation? The result would be an interference with both civil and military aircraft traffic.
5. Does the activity violate any existing international conventions? Yes.
    a. If State A conducts either method to destroy with this radar facility from State B's territorial waters, it would violate the United Nations Convention on the Law of the Sea (UNCLOS III): Art. 17 – Ships of all states enjoy innocent passage through the territorial sea and Art 19 -

Passage is innocent so long as it is not prejudicial to coastal state. Any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State.

b. If State A uses its satellite to conduct information operation it would violate the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space , including the Moon and other Celestial Bodies (Outer Space Treaty): the Preamble - by using space for non-peaceful purpose; Art III – by carrying on activities in space not in accordance with international law: anticipatory self-defense may be considered in contravention of the UN Charter.

c. If State A uses its satellite to conduct the information operation is would violate the Convention on International Liability for Damage Caused by Space Objects (Liability Convention): Art I – damage defines as "loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations" and does not limit how the space object causes damage – thus, by using the satellite to destroy the radar control site the satellite causes the damage and State A would be liable under Art II. If State A's claim of anticipatory self-defense is legitimate, and it acted in accordance with international law, then its liability may be exonerated in accordance with Article VI of the Liability Convention.

d. Destroying the air control radar on the border by either method will have an effect on both military and civil aircraft using the radar system: may cause them to crash without the radar. Such action would violate the Convention on International Civil Aviation (Chicago Convention): Art *3bis* – "every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of person on board and the safety of aircraft must not be endangered." State A would be liable for the injuries, deaths, and property destruction caused as a result of its activities.

6. Does the activity violate any domestic laws or agreements? No.

7. Does the activity cross the proscriptive threshold of use of force of article 2(4) of the UN Charter? If State A's claim of anticipatory self-defense is not accepted under Article 51, then this action would rise to the level of use of force under article 2(4).

7.a. If it was authorized by the Chapter VII authority of the UN Security Council, then the fundamental principles that reflect customary international law apply to information operations that amount to the use of force under Article 41 of the UN Charter during UN operations in which member states are not parties to an international armed conflict. If member states are parties to an international armed conflict, then law of armed conflict applies. No Chapter VII action here.

7.b. If it was not authorized by Chapter VII authority of UN Security Council, the use of force may nevertheless still be authorized under the inherent right of individual or collective self-defense as recognized by Article 51 of the UN Charter. Regardless of whether the use of force is legitimate self-defense, the law of armed conflict applies once State A takes its action. State A asserts that its inherent right of self

defense includes the right to repel preemptively an imminent threat of use of force such as State B's anticipated imminent air raid. Such self-defense measures must be proportionate. State A argues that destroying State B's ability to fly its aircraft by destroying the radar facility is proportionate. State A also asserts that there would be less damage by grounding the force with electronic means than conventional bombs. If State A's self-defense claim is accepted, then the law of armed conflict will be applied to these activities.

B. Armed Conflict and Wartime usage of Information Warfare. Yes, if State A anticipated an imminent attack by State B and State A acted in self-defense.

1. What occurred? State A would destroy State B's radar control facility to ground State B's aircraft and prevent imminent air attack by State B.
2. Determine the identity of the actor. State A, state actor.
3. What was actor's intent behind the information operation? Self-defense.
4. What was result of actor's information operation? Both military and civilian aircraft would be affected.
5. Does the activity rise to the proscriptive threshold of article 2(4) of the UN Charter? No. This would be an act of self-defense under Article 51.
6. Is the conflict an international armed conflict under Common Article 2 of the Geneva Conventions of 12 August 1949 or an internal armed conflict under Common Article 3 of the Geneva Conventions of 12 August 1949. International Armed Conflict.
7. Does the activity affect any state's rights under international conventions? Unknown at this time.
8. Does the activity violate any international conventions or treaties? Note that under the Liability Convention, when State A's act of anticipatory self-defense is within the bounds of international law, State A may be exonerated from liability under this convention.
9. Does the activity comply with Law of Armed Conflict? Yes.
    a. Hague Conventions
        (1) Regulations Respecting the Laws and Customs of War on Land, annexed to Hague convention No. IV Respecting the Laws and Customs of War on Land: No violations noted.
        (2) Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land: not applicable here.
        (3) The 1949 Geneva Convention Number IV Relative to the Protection of Civilian Persons in Time of War: no destruction of civilian property.
    b. Customary international law

State A's actions must comply with the Annexed Regulations to the 1907 Hague Regulation No. IV, Art 22: right of belligerents to adopt means of injuring the enemy is not unlimited. Before State A destroys the radar facilities, it must balance the principles of military necessity and unnecessary suffering: the military necessity of destroying the radar facility and the unnecessary suffering which may not be caused by any air craft which may crash as a result of the lost radar facility. If State A determines that the

> military necessity is required for the partial or complete submission of State B's air force, it must seek to do so with a minimum expenditure of time, life, and physical resources. Nevertheless, it is not unlawful to cause incidental injury or death to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military objective. State A could proceed with either the conventional raid or the information operation to destroy the radar site. The information operation would probably cause less damage. State A should also conduct such operation when there is as little as possible civil aircraft use of that radar facility.

b. *Discussion of Scenario Delta Based on the Analysis Framework* --State A can destroy the radar site by two methods: conventional means or an information operation. The net effect principle for either method is the same: State A's intent behind launching either of the two operations is anticipatory self-defense and the resultant effect will be the destruction of the air radar control facility and grounding of State B's air force. If State A's anticipatory self-defense argument is accepted, then the analysis is carried out under an armed conflict/wartime operation analysis. If it is not, then the analysis proceeds under a peacetime/crisis environment model.

State A's anticipatory self-defense argument may not be accepted for several reasons. Some countries take the view that the customary law right of self-defense to repel imminent armed attacks, not just actual armed attacks, is much broader that the self-defense concept found in Article 51 of the UN Charter which specifically references "if an armed attack occurs." Thus, anticipatory self-defense no longer exists. Many other nations, including the United States, however, assert that the inherent right of self-defense, including anticipatory self-defense, still exists because it is in inherent right of sovereign nations which was never negotiated away in the UN Charter. Therefore, a claim of anticipatory self-defense, based on Secretary of State Webster's writings in *The Caroline*, must meet three

specific criteria: (1) the threat in issue must be imminent/immediate; (2) the action taken must be necessary (no viable alternative); and (3) the force used must be proportionate to the threat posed.

If State A's claim in not accepted, then the analysis proceeds according to a peacetime environment framework. Although both methods to destroy the radar could be used, it appears that use of an information operation would encounter more legal impediments than a conventional raid. As the framework above indicates, depending on how the information attack was conducted, it may violate several international conventions and treaties. Nevertheless, both methods may violate the Law of the Sea Convention and the Chicago Convention.

If State A's claim is accepted, then the analysis proceeds according to a armed conflict/wartime framework. In this instance, it appears that the use of the information operation would presumably reduce any collateral damage and would require no intrusion of an armed force into State B's physical territory.

5. *Scenario Echo* -- Armed conflict actually breaks out between State A and State B. State B continues to receive critical intelligence on the movements of State A's military forces from a satellite imagery systems operated by State C, a declared neutral in the conflict between State A and State B. What are the legal rights and obligations of the three nations with respect to the satellite imagery being provided by State C to State B?

a. *Analysis of Scenario Echo Using the Analysis Framework* --

A. Peacetime usage of Information Operations – No. Start Analysis at No. 11 below.
1. What occurred?
2. Determine identity of actor.
3. What was actor's intent behind the information operation?
4. What was result of actor's information operation? See § IV below.
5. Does the activity violate any existing international conventions?
B. Armed Conflict and Wartime usage of Information Warfare – Yes.
1. What occurred? State C, a declared neutral, is providing satellite imagery to State B regarding the movement of State A's military forces.
2. Determine the identity of the actor. State C, a state actor.
3. What was actor's intent behind the information operation? State C's intent in providing satellite imagery solely to State B and not to State A is unknown.
4. What was result of actor's information operation? State C's liberty as a neutral State to use telecommunications facilities does not imply the power to use them or permit their use as providing assistant to belligerents on one side only. This is a discriminatory act by State C.
5. Does the activity rise to the proscriptive threshold of article 2(4) of the UN Charter? No.
6. Is the conflict an international armed conflict under Common Article 2 of the Geneva Conventions of 12 August 1949 or an internal armed conflict under Common Article 3 of the Geneva Conventions of 12 August 1949? International armed conflict.
7. Does the activity affect any state's rights under international conventions? No.
8. Does the activity violate any international conventions or treaties? No.
9. Does the activity comply with Law of Armed Conflict? No.
    a. Hague Conventions
        (1) Regulations Respecting the Laws and Customs of War on Land, annexed to Hague convention No. IV Respecting the Laws and Customs of War on Land: not applicable.
        (2) State C's actions are in violation of the Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land:
        (3) Art 8 – a neutral State is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals; and Art 9 – requires that every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Article 8 must be impartially applied by it to both belligerents.

b. *Discussion Scenario Echo Based on the Analysis Framework* --

International law generally permits a neutral nation to continue to allow the use by belligerent nations of communications relay facilities in its territory on a non-discriminatory

basis. There is a strong argument that the generation of critical military intelligence such as satellite imagery goes far beyond this limited privilege into active military support to the belligerent nation. State C accordingly has an obligation to cease such support upon demand by State A. If it does not, State A can take reasonable steps in self-defense to interfere with State B's receipt of the imagery. It should select the least destructive and effective means to do it, such as jamming of State B's signal, or destruction of State B's ground station receiving the signal. Destruction of the satellite would be a very serious action, to be taken on as a last resort, because such action would constitute a serious interference with State C's interests, among others, and because of the likely heavy political cost of committing a hostile act in space in violation of The Outer Space Treaty and the Liability Convention.

6. *Scenario Foxtrot* -- During the armed conflict between State A and State B, State A's military information warriors find out that State B is able to communicate with its forces over the national telephone system. The telephone system serves State B's capital city and its military headquarters. The information warriors at State A's military headquarters, quickly disable State B's telephone system by generating a mass dialing attack by personal computers that overwhelms the system. State A's military leaders admit that they did not consider that shutting down the telephone system would have such a widespread and drastic impact.

a. *Analysis of Scenario Foxtrot Using the Analysis Framework* --

A. Peacetime/Crisis usage of Information Operations - No. Proceed to B below.
1. What occurred?
2. Determine identity of actor.
3. What was actor's intent behind the information operation?
4. What was result of actor's information operation?

Others affected

B. Armed Conflict and Wartime usage of Information Warfare - Yes.

1. What occurred? State A's computer dialing attack disrupted State B's telephone system.

2. Determine the identity of the actor: State A, a state actor.

3. What was actor's intent behind the information operation? This operation removed the communications link for State B's military.

4. What was result of actor's information operation? Military no longer able to communicate. The disruption of the phone system affected the civilian population also. All information which is transmitted via phone lines stopped, i.e., the Internet , stock and commodity exchanges, and news services.

5. Does the activity rise to the proscriptive threshold of article 2(4) of the UN Charter? Yes. State A's intent to disrupt the internal telephone system of State B's military headquarters and capital city, and the havoc caused as a result of the mass dialing attack, reach the level of use of force under article 2(4).

6. Is the conflict an international armed conflict under Common Article 2 of the Geneva Conventions of 12 August 1949 or an internal armed conflict under Common Article 3 of the Geneva Conventions of 12 August 1949? International armed conflict.

7. Does the activity affect any state's rights under international conventions? Yes.

8. Does the activity violate any international conventions or treaties? Yes.

   a. United Nations Convention on the Law of the Sea (UNCLOS III) - not applicable, action taken from land.
   b. State A violated The International Telecommunications Convention of 1982 (Nairobi Convention): Art 35, para 158 - Ground stations must not cause harmful interference; and Art 38, para 164 - Military radio installations must prevent harmful interference as far as possible.
   c. If State A used its satellites to carry out this attack on State B's telephone system, then by using the satellite to interfere in State B, it violated the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space , including the Moon and other Celestial Bodies (Outer Space Treaty): Preamble – Explore and use outer space for peaceful purposes; and Art III - carry on activities in space in accordance with international law, including UN Charter.
   d. By using the telephone lines to carry out this attack, State A violated the Convention on International Liability for Damage Caused by Space Objects (Liability Convention): Art I – damage is defined as "loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations;" does not limit how the space object causes damage – thus, by using the satellite to destroy the radar control site the satellite causes the damage and State A would be liable under Art II.
   e. If State A used the INTELSAT system, it violated the Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT) (commercial ground stations): Preamble – refers to Article I of the Outer Space Treaty which states that "outer space shall be used for

the benefit and in the interests of all countries." Art III(a) - "INTELSAT's prime objective is the provision, on a commercial basis, of the space segment required for international public telecommunication services of high quality and reliability to be available on a non-discriminatory basis to all areas of the world." Art III(d) – "INTELSAT space segment may also, on request and under appropriate terms and conditions, be utilized for the purpose of specialized telecommunications services, either international or domestic, other than for military purposes . . . ."

f. If State a used the INMARSAT system, such action is beyond the scope of permitted military use, and violates the Convention on the International Maritime Satellite Organization (INMARSAT) (maritime mobile stations): Preamble – refers to Article I of the Outer Space Treaty which states that "outer space shall be used for the benefit and in the interests of all countries." Art III – provides that the "organization shall act exclusively for peaceful purposes." See the most recent INMARSAT General Counsel Legal Opinion which allows military use of INMARSAT in specific military operations (UN sanctioned activities, etc).

9. Does the activity comply with Law of Armed Conflict? No.
   a. Hague Conventions
      (1) As it appears that State A did not consider the enormous impact and implications of the mass dialing attack, many of the results of the attack violate the Regulations Respecting the Laws and Customs of War on Land, annexed to Hague convention No. IV Respecting the Laws and Customs of War on Land

   a. Prohibited activities because the effects of the dialing attack were unlimited and indiscriminate. Art 22 - means of injuring the enemy not unlimited; Art 23 – weapons may not cause unnecessary suffering; Art 25 – no attacks on undefended places; Art 27 – no attacks on certain places unless used for military purpose; Art 3 (of the Convention proper) – if violate provisions, may be liable to pay compensation; Art 53 – all appliances adapted . . . for the transmission of news . . . may be seized, even if privately owned, but must restore and pay compensation; and, Art 56 – willful seizure, destruction, or damage done to certain institutions may be made the subject of legal proceedings
      (2) Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land – not applicable here.
      (3) Due of the enormous impact of the attack on personal property, and as State A's military commanders did not seem to take into consideration collateral damage on the civilian population, State A's action violate The 1949 Geneva Convention Number IV Relative to the Protection of Civilian Persons in Time of War: Art 53 – any destruction by the occupying power of real or personal property belonging individually or collectively to private persons, or to the State, or to other public authorities, or to social or cooperative organizations, is prohibited, except where such

destruction is rendered absolutely necessary by military operations.

b. Customary international law – There is clear indication that State A never balanced the principles of military necessity and unnecessary suffering before carrying out the attack on State B. This is a clear violation of customary international law: Annexed Regulations to the 1907 Hague Regulation No. IV, Art 22 – right of belligerents to adopt means of injuring the enemy is not unlimited;" proportionality - balancing between the principles of military necessity and unnecessary suffering, and discrimination - restricts methods, weapons, and targets. Military necessity - only the degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources may be applied. Unnecessary suffering – also known as the principle of humanity, provides that employment of any kind or degree of force not required for the purpose of the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources, is prohibited. Incidental injury and collateral damage - it is not unlawful to cause incidental injury or death to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military objective, however, the effect must be proportionate to the military advantage gained.

b. *Discussion of Scenario Foxtrot Based on the Analysis Framework* --Since the telephone system is used for military communications, there is a legitimate military reason to attack it. Since it is also used for civilian purposes, its destruction would also affect the civilian noncombatant population. The targeteer must make his best estimate of the military advantage to be gained by disabling the telephone system and weigh it against his best estimate of the effect on the civilian population. This might not be significant, since civilian losses from deprivation of telephone service are likely to be much less than from blast and fire from conventional weapons, however, it is not just telephone services that were affected by the computer attack. Everything that relied upon the telephone system was also affected. This means that State A's targeteers needed to consider the total results of disabling the telephone system: the crash of the Internet, the stock and commodities exchanges, the emergency services telephone services, etc., Only if the military advantage gained by

talking out this system outweighs the collateral damage, will such an action meet international approval. State A may still argue that, even as immense at the impact was in the Capital city, it was still better than dropping iron bombs on the headquarters building in the densely populated Capitol city.

C. Merits of the Analysis Framework

Information operations and cyberspace present new challenges for international law, however, they are not insurmountable. We have the legal framework to analyze information operations and we do not need a "new theoretical structure of the law."[265] The incrementalist approach is supportive of this view. By analogy to U.S. domestic law and its wrestling with the First Amendment and cyberspace, Professor Lawrence Lessig of the University of Chicago Law School, points out that cyberspace:

> is not a space that we know, in the sense of a space that we have inhabited. Indeed, in one sense, it is just a pattern of electrons skimming a net of computers, a construct that describes a location where a collection of activity occurs. But described like this, the space could not be understood, or at least it could not be understood by us. It is understood by us only when we put things into it, when we carry into it our own language, when we colonize it, when we domesticate it. It is no accident that we speak of e-mail, or that we describe postings on

[265] Kanuck, *supra* note 6, at 274.

> "electronic bulletin boards," or that we wonder about the dynamics of real-time discussions in "CB-chat" areas. We have no choice but to take control of this space at first with our ordinary terms, if indeed we are to understand it. And it is through a practice of analogy that this occupation occurs.[266]

By analogy, this is similar to the incrementalist view of international law. We can apply the current international law framework to information operations and information warfare based upon our ability to provide analogous understanding of the basic principles of international law. "For like domestic law, international law is not a static body of rules but rather a living creature, continually forged and shaped to serve the needs of an international community that itself is constantly change."[267]

A violation of sovereignty in the visual sense is easy to conceptualize – soldiers or weapons physically entering the territory (territorial seas or airspace) of another nation. What perplexes many today is what happens when a foreign state enters electronically? Is this the same thing and does it have the same effect? How do we apply the current international law paradigm to this new method warfare? By applying an incrementalist approach and the net effect principle.

---

[266] Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1744 (1995).

[267] Robertson, *supra* note 107, at 103.

One has to look past the newness of the methods and past the territorial aspect of sovereignty to find the answer with the current framework. International law has experienced similar events in the past and dealt with them accordingly. Since the advent of the radio, for example, broadcasts into other countries have been looked upon as infringing upon sovereignty.[268] This is because the concept of sovereignty not only includes control over the territory, but independence of action within it.[269] In fact, the United Nations Charter has formalized this aspect protecting both "territorial integrity" and "political independence."[270] While the charter deals with protecting these aspects from the threat or use of force, the underlying premise is "that a sovereign state is accorded the right to shape its cultural, social, and political life as it wishes, ..."[271] Despite this, nations have attempted for a variety of reasons to protect their own interests or the interests of others within the borders of other sovereign states.[272]

---

[268] VON GLAHN, *supra* note 108, at 418-421 (discussing the attempts to control radio communications so that they "avoid interference with the communications services of all contracting a governments or agencies.").

[269] MARK W. JANIS, AN INTRODUCTION TO INTERNATIONAL LAW 122 (1988) (hereinafter JANIS) ("A sovereign state is one that is free to independently govern its own population in its own territory and set its own foreign policy."); LEVI, *infra* note 273, at 91 ("Respect for a state's sovereignty requires that other states do not interfere in its internal affairs, including the internal aspects of foreign policymaking.").

[270] The Charter provides that "[a]ll members hall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state . . . ." U.N. Charter, *supra* note 138, art. 2(4).

[271] ANN VAN WYNEN THOMAS & A.J. THOMAS, JR., THE CONCEPT OF AGGRESSION IN INTERNATIONAL LAW 83 (1972).

[272] *See* WERNER LEVI, CONTEMPORARY INTERNATIONAL LAW: A CONCISE INTRODUCTION 91-99 (1979) (hereinafter LEVI).

As treatises proliferate and the practice of states establish customary norms of behavior in international law, precisely which matters are solely within the internal purview of the state may change.[273] For example, the advent of human rights law has begun a fairly major movement, of which the U.S. has been a part, to intervene in the affairs of other states for humanitarian reasons.[274] As the world becomes more interconnected and American capability to communicate and interact between nations becomes more and more broad based, what states consider "internal" will almost assuredly shrink. Can a nation legally intervene electronically in a communist regime to promote democracy because it feels democracy is better for the people? Can a nation legally jam and superimpose its news over state-sponsored news in another nation because that nation's portrayal of the first state is inaccurate or biased? Without discussing the relative merit of such intervention or its "peaceful purpose," it seems clear that by applying the net affect principle and looking at the actor's intent and the result achieved, these actions violate a strict interpretation of sovereignty, at least defined as territorial integrity and independence of action within that territory.

The use of sovereignty as a legal concept against the U.S. in international law will surely increase as it increases its information capability and use.[275] This cry of foul will most

---

[273] Id., at 91.

[274] *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 703 cmt. E & reporter's note 8 (discussing several theories that are increasingly accepted as authorizing humanitarian intervention.).

[275] Technology has always engendered changes in the international law surrounding sovereignty. For example, sovereignty over airspace was a result of the airplane and the

likely come from those who do not have similar capabilities. It is precisely this type of political usefulness that the concept of sovereignty has been jealously guarded for, despite its diminished power.[276]

We must consider that the U.S. is probably the most vulnerable nation on earth to electronically-based information propaganda.[277] In fact, other governments most often do not need their own assets, they can simply use America's open information sources against it.[278] Thus, we need to rethink and recommit to an enhanced concept of sovereignty. Because of America's vulnerability, strengthening sovereignty as a legal concept between nations helps the U.S. to seek international remedies, short of using elements of its own national power, if another nation attempts to undermine U.S. internal affairs. Still, at the strategic level, protecting U.S. interests may require attempts to influence perceptions in other states. Doing so, however, may subject the nation to legal and political repercussions from the community nations; this is particularly true when U.S. actions may be viewed as aggression or use of force.

---

many telecommunications conventions have been the result of radio and television communications. *See* VON GLAHN, *supra* note 108, at 405 & 418.

[276] *See* LEVI, *supra* note 273, at 99 ("The evidence is clear that states find the survival of sovereignty most useful as a political and legal tool, in full awareness of its drawbacks . . . .").

[277] *Cf.*, TOFFLER, *supra* note 6, at 147-1515 (discussing the vulnerability of U.S. "knowledge" assets); Id. at 208-09 (discussing the power of the media in this country); and Eliot A. Cohen, *A Revolution in Warfare*, FOREIGN AFFAIRS, Mar.-Apr. 1996, at 37 (discussing the vulnerability of the United States, as an information-based society, to information-based attack).

[278] *Cf.* TOFFLER, *supra* note 6, at 175 ("But win, lose, or draw, the media . . . will be a prime weapon for Third Wave combatants in both the wars and anti-wars of the future, a key component of knowledge strategy.").

As discussed above, we do not know everything about information operations, and the knowledge we do possess, is imperfect at best. I assert that we are not currently operating in a "third wave"[279] environment, and we do not know when this will, if ever, occur.[280] In light of the above, I submit that we are experiencing an evolution in technology which has increased and modified in some ways our warfighting capabilities, but has not at this time, changed the overall nature of warfare or the basic nature of the nation state.[281] As such, international law's prior experiences with technology and warfare are extremely useful as we embrace the incrementalist process in analogizing and applying international law to information operations and warfare.

The incrementalist approach allows us to analyze issues which apparently do not fit logically into the current paradigm. We will draw upon knowledge gained from both

---

[279] As used in this discussion, the term "third wave" indicates that society is at a point where it must understand and deal with the nuances of information-based technologies used during conflict. It is not necessarily a complete acceptance of the Tofflers' theories.

[280] Learned scholars in the area of information operations assert that we are not in the "third wave" yet. They maintain that the world is really operating in an environment that is a combination of the first, second, and third waves systems. Interview with Dr. John I. Alger, Dean, School of Information Warfare Strategy, National Defense University, in Ft. McNair, Washington, D.C. (Jan. 31, 1997); Interview with Dr. Fredrick Giessler, Professor, School of Information Warfare Strategy, National Defense University, in Ft. McNair, Washington, D.C. (Mar. 3, 1997); and Interview with Dr. Daniel Kuehl, Professor, School of Information Warfare Strategy, National Defense University in Ft. McNair, Washington, D.C. (Jan. 31, 1997).

[281] The military has used the term "intelligence preparation of the battlefield" (IPB) to describe those operations used to develop a detailed knowledge of the adversary's information systems. *See* FM 100-6, *supra* note 5, at 4-4. It is interesting to note that the current term used at the Joint Chiefs of Staff Level for IPB is the more all-encompassing and more futuristic term "battlespace." JCS PUB. 1-02, *supra* note 58, at 194.

previous similar and dissimilar experiences shared under that framework. Such synthesis of the old and the new results in the use of a current model with minimal, if any, changes to the framework. It serves to protect the basic tenets of international law.

By engaging in an incrementalist process concerning information operations rather than a maximalist approach which would creature a completely new legal structure, the application of the current framework will not produce perfect results. Some gaps in coverage may appear at first, particularly when applying treatises and customary international law which developed many years before the concept of information operations. Such problems include the current inability to identify the actor every time or the inability to predict and assess accurately damage from such operations. However, this is a problem with conventional operations, such as when covert operations are used or certain facts are unknown about potential targets for conventional bombs. These problems merely force more careful scrutiny of such offensive operations.

Nevertheless, certain basis concepts and principles such as sovereignty, military necessity, proportionality, and chivalry, can be analogized and applied successfully. Information operations and warfare have not obliterated these basic tenets of international law. How we apply these principles to information operations will continue to develop and improve as our understanding of information operations continues to advance. As in the past, as the world community's experiences with information operations and warfare grows, so to will the world community's ability to agree on certain standards to apply to information operations. Overtime, these may develop into customary international law on this topic.

Moreover, as nations experience information operations, they may seek consensus through the treaty making process. All of this can occur within the current international law paradigm and does not require a new theoretical structure of the law.

V. Conclusion.

Advances in information-based technology is changing how we process and use information in the Information Age. Information operations and information warfare fit within our current legal paradigm. They do not fit perfectly, however, because the nature of warfare has not changed, and information operations and information warfare still fall under the basic principles of international law such as use of force, proportionality and discrimination. By using the net effect principle, and by applying an incrementalist perspective to these operations, the current international legal framework is applicable to "the war out there that is not about bullets, but who controls the information: what we see, how we work, what we think. It is really all about the information."

APPENDIX A

FRAMEWORK OF ANALYSIS UNDER CURRENT LEGAL PARADIGM

The following is a framework to determine the legality of an information operation/warfare activity under international law

A. Peacetime usage of Information Operations
   1. What occurred? What technique was employed? See § C below.
   2. Determine identity of actor.
      a. State Actor – proceed with analysis
      b. State-sponsored actor – proceed with analysis
      c. Non-State Actor - do not proceed with analysis; look to criminal and civil analysis frameworks
      d. Unable to identify – attempt to proceed with this analysis
   3. What was actor's intent behind the information operation?
      a. Criminal
      b. Interference in national sovereignty
      c. Self-defense
      d. Accident
   4. What was result of actor's information operation?
      a. Military affected
      b. Civilian population affected
      c. Others affected
   5. Does the activity violate any existing international conventions?
      a. United Nations Convention on the Law of the Sea (UNCLOS III)
         (1) Art. 17 – Ships of all states enjoy innocent passage through the territorial sea
         (2) Art 19 - Passage in innocent so long as it is not prejudicial to coastal state
         (3) Art 109 – Unauthorized broadcasting from high seas
      b. The International Telecommunications Convention of 1982 (Nairobi Convention)
         (1) Art 19, para 132 - Stop transmissions of private telegrams which threaten security of State
         (2) Art 19, para 133 - Cut off private telecommunications which threaten security of State
         (3) Art 20, para 134 - Suspend international telecommunication service
         (4) Art 35, para 158 - Ground stations must not cause harmful interference
         (5) Art 38, para 164 - Military radio installations must prevent harmful interference as far as possible
      c. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space , including the Moon and other Celestial Bodies (Outer Space Treaty)
         (1) Preamble – Explore and use outer space for peaceful purposes.

(2) Art III - carry on activities in space in accordance with international law, including UN Charter
(3) Art IV - No nuclear weapons or weapons of mass destruction in space; only use moon for peaceful purposes

d. Convention on International Liability for Damage Caused by Space Objects (Liability Convention)
(1) Art II – launching state liable to pay compensation for damage cause by its space object on the surface of earth or aircraft flight.
(2) Art I – damage defined as "loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations."

e. Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT) (commercial ground stations)
(1) Preamble – refers to Article I of the Outer Space Treaty which states that "outer space shall be used for the benefit and in the interests of all countries."
(2) Art III(a) - "prime objective the provision, on a commercial basis, of the space segment required for international public telecommunication services of high quality and reliability to be available on a non-discriminatory basis to all areas of the world."
(3) Art III(d) – "INTELSAT space segment may also, on request and under appropriate terms and conditions, be utilized for the purpose of specialized telecommunications services, either international or domestic, other than for military purposes . . . ."

e. Convention on the International Maritime Satellite Organization (INMARSAT) (maritime mobile stations)
(1) Preamble – refers to Article I of the Outer Space Treaty which states that "outer space shall be used for the benefit and in the interests of all countries."
(2) Art III – provides that the "organization shall act exclusively for peaceful purposes."
(3) See most recent INMARSAT General Counsel Legal Opinion which allows military use of INMARSAT in specific military operations (UN sanctioned etc)

f. Convention on International Civil Aviation (Chicago Convention)
(1) Art *3 bis* – "every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of person on board and the safety of aircraft must not be endangered."
(2) United States position on Art *3 bis:* it applies as a matter of customary international law.

6. Does the activity violate any domestic laws or agreements?
a. Espionage Laws

b. Executive Order 12333 – United States Intelligence Activities
c. Covert Actions – 50 U.S.C. 413b(e)
d. Traditional Military Activities – 50 U.S.C. 413e
e. Telecommunications Contracts with commercial companies

7. Does the activity crosses the proscriptive threshold of use of force of article 2(4) of the UN Charter?
   a. If it was authorized by the Chapter VII authority of the UN Security Council, then the fundamental principles that reflect customary international law apply to information operations that amount to the use of force under Article 41 of the UN Charter during UN operations in which member states are not parties to an international armed conflict. If member states are parties to an international armed conflict, then law of armed conflict applies.
   b. If it was not authorized by Chapter VII authority of UN Security Council, the use of force may nevertheless still be authorized under the inherent right of individual or collective self-defense as recognized by Article 51 of the UN Charter. Regardless of whether the use of force is legitimate self-defense, the law of armed conflict applies.

B. Armed Conflict and Wartime usage of Information Warfare
   1. What occurred? What technique was employed? See § C below.
   2. Determine the identity of the actor.
      a. State Actor – proceed with this analysis
      b. State-sponsored actor – proceed with this analysis
      c. Non-State Actor - do not proceed with analysis; look to criminal and civil analysis frameworks
      d. Unable to identify – attempt to proceed with this analysis
   3. What was actor's intent behind the information operation?
      a. Criminal
      b. Interference in national sovereignty
      c. Self-defense
      d. Accident
   4. What was result of actor's information operation?
      a. Military affected
      b. Civilian population affected
      c. Others affected
   5. Does the activity rise to the proscriptive threshold of article 2(4) of the UN Charter?
   6. Is the conflict an international armed conflict under Common Article 2 of the Geneva Conventions of 12 August 1949 or an internal armed conflict under Common Article 3 of the Geneva Conventions of 12 August 1949?
   7. Does the activity affect any state's rights under international conventions? Multilateral conventions:
      a. Vis-à-vis parties to the conflict: absent a specific termination or suspension clause, the obligations of a treaty may continue to exist

between treaty parties that are not a party to an armed conflict depending upon the intrinsic character of the treaty.

b. Vis-à-vis non-parties to the conflict:
   (1) belligerent state has the duty under the law of war to respect the rights of neutral states and vice versa.
   (2) Contractual obligations imposed by convention may be modified by specific terms of the convention, general principles of treaty termination or suspension, and operation of Article 103 of the UN Charter.

8. Does the activity violate any international conventions or treaties?
   a. United Nations Convention on the Law of the Sea (UNCLOS III)
   b. The International Telecommunications Convention of 1982 (Nairobi Convention)
   c. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space , including the Moon and other Celestial Bodies (Outer Space Treaty)
   d. Convention on International Liability for Damage Caused by Space Objects
   e. Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT)
   f. Convention on the International Maritime Satellite Organization (INMARSAT)
   g. Convention on International Civil Aviation (Chicago Convention)
9. Does the activity comply with Law of Armed Conflict?
   a. Hague Conventions
      (1) Regulations Respecting the Laws and Customs of War on Land, annexed to Hague convention No. IV Respecting the Laws and Customs of War on Land
         (a) Prohibited activities
            (i) Art 22 - means of injuring the enemy not unlimited
            (ii) Art 23 – weapons may not cause unnecessary suffering
            (iii) Art 25 – no attacks on undefended places
            (iv) Art 27 – no attacks on certain places unless used for military purpose
         (b) Permitted Activities
            (i) Art 24 - ruses of war
            (ii) Art 53 – Army of occupation and seizure of cash, funds, and realizable securities which are strictly state property
         (c) Liabilities
            (i) Art 3 (of the Convention proper) – if violate provisions, may be liable to pay compensation.

(ii) Art 53 – all appliances adapted . . . for the transmission of news . . . may be seized, even if privately owned, but must restore and pay compensation.

(iii) Art 56 – willful seizure, destruction, or damage done to certain institutions may be made the subject of legal proceedings

(2) Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land

(a) Prohibited Activities

(i) Art 3 – prohibits belligerents from erecting on a neutral state's territory a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea; or using any similar installation previously established by the belligerents on the land of a neutral for purely military purposes

(ii) Art 5 – prohibits neutral state from allowing any acts referred to in 2 and 4 from occurring on its territory

(b) Permitted Activities

(i) Art 8 – a neutral State is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.

(ii) Art 9 – requires that every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Article 8 must be impartially applied by it to both belligerents.

(c) Liabilities – a neutral state that is not acting under the authority of the UN Security Council will lose its neutrality if it commits a hostile act against a belligerent or it is commits an act in favor of a belligerent.

b. The 1949 Geneva Convention Number IV Relative to the Protection of Civilian Persons in Time of War

(1) Prohibited Activities - Art 53 – any destruction by the occupying power of real or personal property belonging individually or collectively to private persons, or to the State, or to other public authorities, or to social or cooperative organizations, is prohibited, except where such destruction is rendered absolutely necessary by military operations.

(2) Liabilities

(a) Art 147 – "Grave breaches . . . shall be those involving . . .extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly."

(b) Art 148 – "No High Contracting Party shall be allowed to absolve itself or any other High Contracting Party of any liability incurred by itself or by another High Contracting Party in respect of breaches referred to in the preceding Article."

c. Customary international law

(1) Annexed Regulations to the 1907 Hague Regulation No. IV, Art 22 – right of belligerents to adopt means of injuring the enemy is not unlimited."

(a) proportionality - balancing between the principles of military necessity and unnecessary suffering

(b) discrimination - restricts methods, weapons, and targets.

(2) Military necessity - only the degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources may be applied.

(3) Unnecessary suffering – also known as the principle of humanity, provides that employment of any kind or degree of force not required for the purpose of the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources, is prohibited.

(4) Chivalry – forbids treacherous means, dishonorable expedients, and dishonorable conduct during armed conflict; implemented through provisions which concern perfidy and ruses of war.

(5) Incidental injury and collateral damage - it is not unlawful to cause incidental injury or death to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military objective.

C. Type of Information Operation/Warfare Techniques Available

1. Worms
2. Viruses
3. Logic bombs
4. Trojan horses
5. Fund transfers
6. Electronic warfare
7. Data stream corruption
8. Electronic jamming and broadcasting

9. Electromagnetic pulse devices (EMP)
10. Data collection (sniffing/cracking)
11. Booby trapped computer chips in weapon systems or due use systems
12. Interference with air traffic control facilities or GPS navigation systems
13. Destruction of C2 systems that include hospital records or emergency dispatch Systems
14. Complete or partial denial or destruction of national information-transfer media or of transborder data flow (TBDF)
15. Corruption, manipulation, or destruction of financial system database.